BİLGİ SİSTEMLERİ ve BİLİŞİM YÖNETİMİ

Beklentiler ve Yeni Yaklaşımlar



Editörler

Prof. Dr. Fahrettin ÖZDEMİRCİ
Uzm. Zeynep AKDOĞAN



Ankara Üniversitesi Doğal Sit Alanı Beşevler Merkez Yerleşkesinde korunması ve üretilmesi için alan tahsis edilmiştir.



*Beypazarı Geveni
Astragalus Beypazaricus

Ankara-2017

T.C.
ANKARA ÜNİVERSİTESİ
BİLGİ YÖNETİM SİSTEMLERİ BELGELENDİRME MERKEZİ (BİL-BEM)

BİLGİ SİSTEMLERİ ve BİLİŞİM YÖNETİMİ
Beklentiler ve Yeni Yaklaşımlar

Editörler

Prof. Dr. Fahrettin ÖZDEMİRCİ
Uzm. Zeynep AKDOĞAN

Ankara- 2017

ISBN: 978-605-61009-8-7
e.ISBN: : 978-605-61009-9-4

1.Baskı: Ankara, 2017

Para ile Satılmaz. Ankara Üniversitesi Açık Erişim Sisteminden erişilebilir. Ayrıca http://bilbem.ankara.edu.tr ve http://ebeyas.org adreslerinden de erişiebilir.

Bilgi sistemleri ve bilişim yönetimi: Beklentiler ve yeni yaklaşımlar/ Editörler Fahrettin Özdemirci, Zeynep Akdoğan.- -Ankara, 2017.
xiii, 331 s.: res,tbl., şkl, grf ; 16x23,5 cm.

ISBN 978-605-61009-8-7
e- ISBN 978-605-61009-9-4
Kaynakça var.

1.Elektronik Belge Yönetimi. 2. e-Arşiv. 3. Bilgi Sistemleri. 4. Bilişim Yönetim. 5. Yeni Teknolojiler ve Güvenlik. 6. Kişisel Verilerin Korunması
I.Özdemirci, Fahrettin. II. Akdoğan, Zeynep.

Baskı Yeri:
Ankara Üniversitesi Basımevi
İncitaşı Sokak No.10, 06510, Beşevler/ANKARA
Tel: 0312-213 66 55
Basım Tarihi: 29.12.2017

Kitapta yer alan çalışmalar çifte körleme yöntemiyle Bilim Kurulu tarafından değerlendirilmiştir.

İçindekiler

2. BÖLÜM

YENİ TEKNOLOJİLER, GÜVENLİK VE HUKUK

3. BÖLÜM EBYS UYGULAMALARININ BOYUTLARI VE STANDARTLAR

Editörden…

Erişemediğiniz bilgi sizin değildir.
Bilgi sistemleri ve bilişim yönetimi bilgiye erişiminizi sağlar.

Bilgi varlıklarının katma değere dönüştürülmesi çağımızın önemli konularından birisidir. Tüm sektörlerde olduğu gibi kamu sektörü bilgisinin ekonomik değeri yeniden kullanım çerçevesinde şekillenmektedir. Verilerin üretimi, bilgiye dönüşümü ve bilginin karar süreçlerinde kullanımı ekonomik değer süreci ile ele alınmalıdır.

Kamu bilgisinin üretilmesi bir harcamayı gerektiriyorsa ticari boyutu var demektir. Ekonomide kamu ve özel firmaların rollerinin değişmesi ile birlikte kamu sektörü bilgilerinin yeniden kullanımına yönelik pazar genişlemektedir. Teknolojik yenilikler, özellikle mobil ağların gelişmesi, birçok alanda kamu sektörü bilgisi tabanlı hizmetlerin gelişmesini beraberinde getirmektedir. Bilgi üretiminde en büyük paya sahip olan kamu sektörünün bilgi ekonomisinde **yarattığı pay ve değerin ölçeklenebilir ve ölçülebilir** sistemlere kavuşturulması gerekir.

Bu bağlamda, bilgi sistemleri ve bilişim yönetiminde ihtiyaç duyulan ürünlerin ve yazılımların standartlara uygunluğunun sertifikalandırılması yetmemekte; kurumların bilgi sistemi süreçlerini yönetebilme yeteneği, iş ve işlem süreçlerini e-ortamda yürütme becerisi ve başarısı, bilgi sistemlerini kullanma yetkiliğinin ölçülmesi ve sertifikalandırılması gerekmektedir. Bilgi ve iletişim teknolojilerini üretme ve kullanma beceri ve yeteneğinin yüksek olduğu toplumların, devletlerin, kurumların geleceği şekillendireceği, diğerlerinin ise **var olma mücadelesinde yok olma riskiyle karşı karşıya kalacağı bir dönemden geçiyoruz**.

Bu çerçevede; bilgi sistemlerinin ve bilişim yönetiminin bir kurumda etkin olması: iki temel unsura bağlıdır. **Birincisi**, etkin kurumsal yapılar; **ikincisi**, yetki ve sorumluluklardır. Bu unsurlar net olarak ortaya konulmadan bilgi yönetimi ve bilişim sistemleri bir kurumda etkin olarak yönetilememekte; en iyi, en nitelikli olarak tanımlanan yazılımlara sahip olmak yetmemektedir. Konuyu bir bütün olarak görebilmek için öncelikle meselelerin hayatımıza girişi, getirdikleri, götürdükleri konusunda bilgi sahibi olmak, getirdiklerinin kaos veya düzen oluşturup oluşturmayacağı konusunda kafalarda sorulara yer açmak gerekmektedir.

Bugün farklı disiplinlerde kullanılan ve çoğu artık ortak olan, ancak farklı boyutları ile tanımlanan, anlam yüklenen kavramlardan bazılarını burada sıralamakta yarar olduğunu düşünüyorum. Amaç bu alanda çalışanların ve

çalışmayı düşünenlerin bu kavramları bilerek, birbiriyle ilişkilendirerek kendilerini geliştirmeleri ve çalışmalarını sürdürmeleri içindir. Bu yaklaşım farkı disiplinlerle neden birlikte çalışılması gerektiğinin de daha iyi anlaşılmasını sağlayacaktır.

- **e-Dünya** – e-Bağımsızlık – **e-Mahremiyet** – e- Güvenlik
- Dijital bellek - **Yapay zeka** - Dijital bilinç - **Endüstri 4.0**
- **Kurumsal bellek** – Arşiv – **Kurum veri merkezi-** Felaketten kurtarma merkezi
- Sistemlerin evrimi - **Sistemlerin DNA'sı** - Kendini yenileyen sistemler
- **Siber güvenlik** - Siber terörizm - **Veri ve bilgi güvenliği**
- e-Kurum - **e-Devlet** -Bulut bilişim
- **e-Ortamlar ve büyük veri** - Yapılandırılmamış veri - **Anomali analizi**
- Gerçek zamanlı veri analizi - **Hareket analizleri-** Verinin/bilginin kıymetlendirilmesi
- **Ölçeklenebilir veri** - Ölçülebilir veri noktaları oluşturma
- Kişisel veri – **Veri noktalarından kişilik analizleri oluşturma** - Kişi/kişilik profili oluşturma
- **Kurumsal veri** - Veri noktalarından kurum analizleri oluşturma - **Kurum profili oluşturma**
- Açık devlet verisi- **Açık kamu verisi-** Veri koruma hukuku

Tüm bu kavramlar ve olgular **bilgi sistemleri ve bilişim yönetiminin** odak noktalarını oluşturmaktadır.

Bilgi yöneticileri ile bilişimcilerin birlikte çalışması, alanı ileri götürmek için şarttır. Bilginin e-ortamda etkin, güvenilir üretimi ve yönetimi, işbirliklerinin yapılmasını, deneyimlerin paylaşılmasını gerektirmektedir. Kuşkusuz deneyim vardığımız yer değil, gittiğimiz yol olmalıdır. Yolda yaşadıklarımız, bizi değiştirecek ve geliştirecektir. Eğer yolculuğa dikkat edersek, işbirliklerimizi artırırsak, deneyimlerimizi paylaşırsak ancak o zaman gelişebileceğiz.

Birbirleriyle kıyaslanabilir nitelikte olmayan sonuçları bir cadı kazanına atıp karıştırmaktan ibaret bir disiplinlerarası yaklaşımdan kaçınmak da gerekir. Ülkemizde çok değerli yazılımcılar var, ancak kurguya da ihtiyaç var, sistematize etmeye de ihtiyaç var. Biz bunları yapabilirsek, ihtiyaçlarımızı ortaya koyabilirsek, **yerli yazılımların niteliği artacaktır**. Küreselleşen dünyada buna daha çok ihtiyacımız var, oyun kurucu olmak için buna ihtiyacımız var, artık **sihirli değnek kod yazabilmekte, yazılım yapabilmekte, etkin olarak yönetebilmektedir.** Günümüzde modern organizasyonların varlığı özgürleşmeye

dayalıdır. Artık özgürleşme, **yönetim süreçlerinin yönetildiği yazılımların milli olmasından** geçmektedir. Yönetilir ve yönlendirilebilir kullanıcı mı olacağız, yoksa yöneten ve yönlendiren mi olacağız? **e-Bağımsızlık için** evrensel standartlara uygun **yerli yazılımlar, yerli bilgi sistemleri** hedefimiz olmalıdır.

Kurumlar bundan 10, 20, 50, 100 yıl sonra kendilerini nerede görmek istiyorlar? Yol haritalarını ona göre çizecekler, bilgi sistemlerini ona göre şekillendirecekler. Bilgi sistemleri ve bilişim yönetimi kurumlarımızın, toplumumuzun, devletimizin geleceğidir.

Artık elektronik belge yönetimi ve elektronik arşivler bilgi sistemlerinin ve bilişim yönetiminin en önemli ve en büyük alanını oluşturmaya başlamış, bilgi sistemlerin baş aktörü haline gelmiştir. Elektronik belge yönetimi ve e-arşiv uygulamaları, e-imzanın kullanımını hızla yaygınlaştırmış, güvenli belge-bilgi üretmenin ve paylaşmanın en güzel örneklerini oluşturmuştur.

Bilgi ve belge yönetimi alanının da, yeni gerçeklerini tespit edip kendine güncel ve vizyoner bir yol haritası çizerek hızla gelişip evrilmesi gerekmektedir. Bilgi sistemlerinde, bilgi üretiminde, kullanımında yaşanan değişim, bilgi ve belge yönetimi bölümlerinin kabına sığmamasına neden olmaktadır. Bilgili olmak başarılı olmak anlamına gelmemekte; başarı, bilginin etkin kullanımını ve yönetimini gerektirmektedir. Artık etki alanı genişleyen ve değişen Bilgi ve Belge Yönetimi Bölümleri kendilerine daha geniş hareket alanı aramak durumuna gelmiştir.

Kapsama alanı, etkileri çok geniş ve çok çok uzun soluklu olan bilgi sistemleri ve bilişim yönetimi uygulamalarının geliştirilmesinde, yönetilmesinde ve kullanımında bilgi/belge yöneticileri, bilişimciler, bilgisayar mühendisleri, yazılım mühendisleri, yönetim bilimciler birlikte çalışmalıdır.

Bu yayında yer alan çalışmalar, disiplinlerarası yaklaşımla 19-20 Ekim 2017 tarihleri arasında Ankara Üniversitesi Bilgi Yönetim Sistemleri Belgelendirme Merkezi (BİL-BEM), Belge Yönetimi ve Arşiv Sistemi (BEYAS) Koordinatörlüğü, Bilgi İşlem Daire Başkanlığı tarafından düzenlenen ve TÜRKSAT ana sponsorluğunda gerçekleştirilen "Kurumsal Dinamikler Çerçevesine Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar Sempozyumu"nda sözlü olarak sunulan bildirilerden bağımsız birer çalışmaya dönüştürülen ve genişletilen makalelerden oluşmaktadır. Bağımsız çalışmalar, çift körleme yöntemi ile hakem değerlendirmesinden geçirilerek bu kitapta yayınlanmıştır.

Kitapta ele alınan konuları Endüstri 4.0'ın bir parçası olarak değerlendiriyoruz. Çünkü biz Endüstri 4.0 devrini yaşıyoruz ve bunun ne kadar farkındayız! Endüstri 4.0 disiplinlerarası çalışmaları gerektiren bir kapsama sahiptir ve disiplinlerin birbirinden öğrenecek çok şeyleri olduğu çağımızın da bir gerçeğidir. Endüstri 4.0

başlığı altında yapay zeka gibi ileri düzey uygulamalar **insanlığı şekillendirmektedir**. Her geçen gün kurumlarda, toplumlarda, **devletlerde veri işlemede yapay zekâ ve robotik sistemler** önem kazanmaktadır.

Kitapta yer alan çalışmalarda, bilgi sistemleri ve bilişim yönetimi konuları yenilikçi yaklaşımlarla, farklı disiplinlerin bakış açılarıyla, farklı boyutlarıyla, uygulama örnekleriyle ele alınmakta ve değerlendirilmektedir. Bu bağlamda Kitapta yer alan 21 değerli çalışma üç başlık altında gruplandırılarak araştırmacılara ve okuyuculara sunulmaktadır. "**Elektronik Belge-Bilgi-Arşiv ve Açık Devlet Verisi, Büyük Veri, Yapay Zeka Üzerine Yeni Yaklaşımlar**" başlıklı **Birinci Bölümde**; elektronik belge-bilgi-arşiv sistemleri ile açık devlet verisi, büyük veri, yapay zekâ konularına ilişkin yeni yaklaşımları, çözümlere yönelik yeni bakış açılarını ve değerlendirmeleri içeren çalışmalara yer verilmektedir. "**Yeni Teknolojiler, Güvenlik ve Hukuk**" başlıklı **İkinci Bölümde**; elektronik belge-bilgi-arşiv sistemlerinin teknik altyapı, yeni teknolojiler, felaket yönetimi, güvenlik, kişisel verilerin korunması ve hukuk boyutuna açıklık getiren araştırmalar bize önemli bilgiler sunmaktadır. "**EBYS Uygulamalarının Boyutları ve Standartlar**" başlıklı **Üçüncü Bölümde**; kurumsal deneyimler ve uygulama örnekleri bağlamında e-belge-bilgi-arşiv yönetim sistemi uygulamalarının boyutu, gerekli standartlar, standartların getirdikleri, nitelikli insan gücü gereksinimi ve yetiştirilmesine ilişkin çalışmalar yer almaktadır.

Kitap basılı ve elektronik olarak yayınlanmaktadır. Kitap para ile satılmamaktadır. e-Kitap Ankara Üniversitesi Açık Erişim Veritabanı'nda yer almaktadır. Ayrıca; BİL-BEM Web (http://bibem.ankara.edu.tr), Fahrettin Özdemirci Web (http://fahrettinozdemirci.com.tr), e-BEYAS Sempozyumları Web (http://ebeyas.org) sitelerinden erişilebilmektedir.

Ankara Üniversite Bilgi Yönetim Sistemleri Belgelendirme Merkezi (BİL-BEM) olarak TÜBİTAK ULAKBİM DergiPark platformunda "**Bilgi Yönetimi**" adıyla bilimsel elektronik dergi çıkarmak için başvuru yapılmış ve DergiPark'ta açılmıştır. Bilgi Yönetimi Dergisine http://dergipark.gov.tr/by adresinden erişebilirsiniz. Bilgi Yönetimi Dergisi ilk sayısını Haziran 2018 de çıkarmak için çalışmalara başlamıştır. Bu bağlamda tüm araştırmacılarımızın ve okurlarımızın dergiye katkı vermelerinden memnuniyet duyacağımız belirtmek isteriz.

Bu alanda literatürün zenginleştirilmesine katkı sağlayan tüm yazarlara ve çalışmaları değerlendirerek, öneriler sunarak çalışmalara katkı sağlayan Bilim Kurulu üyelerinize teşekkür ederiz.

Saygılarımla,
Fahrettin Özdemirci
Editör, BİL-BEM Müdürü
Gölbaşı Aralık 2017

1. BÖLÜM

ELEKTRONİK BELGE-BİLGİ-ARŞİV VE AÇIK DEVLET VERİSİ, BÜYÜK VERİ, YAPAY ZEKA ÜZERİNE YENİ YAKLAŞIMLAR

Bilginin Bilgiyle Savaşı: Belge/Bilgi Yönetimi Vizyonuyla İstihbarat

Mehmet TORUNLAR
T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü

Öz

Günümüze çok uzak olmayan bir geçmişte "bilgi ve bilginin kontrolü" insanların hayatında yeni gerçeklik olarak devreye girmiştir ve bu her şeyi değiştirdiği gibi insanın algılamalarını da değiştirmekte, insana has algılama yetisi makinelere devredilmekte, makine algılamaları üzerinden mücadelelere girişilmektedir. Bunu da insanoğlu düşünerek, planlayarak ve kendi elleriyle gerçekleştirmektedir. Bugün bu alandaki mücadele, egemenlik kurma faaliyetleri hızla devam etmekte, "bilgi çağı/ekonomisi/toplumu/savaşı" denen olgu bir takım yeni gerçeklik ve yoğun metamorfik etkilerle, "Endüstri 4.0" başlığı altında "yapay zekâ" gibi ileri düzey uygulamalarla insanlığı (farkında olalım veya olmayalım) şekillendirmektedir. Günümüzde bu değişimin çok belirgin, formel veya doktrinel bir tanımlaması henüz belki mevcut değildir. Elbette hayatın her alanını ve birey birey herkesi etkilediği gibi istihbarat alanını da etkilediği söylenmelidir. Çok uzak olmayan gelecek zamanda da asli jargon bilgisayar ve ürünleri ile iletişim olgusu temelinde sürecektir ve dünya yine bilgiyi elde etme, ele geçirme, kontrol altında tutma mücadelesi olarak şekillenecek gibi görülmektedir. Ancak bu yeni gerçeklikte bilginin bilgiyle savaşı ana ekseninde hayata devam edebilme çabası daha sert ve çetrefilli olacak, "insan-makine-yapay zekâ" mücadelenin başrol oyuncuları olacaktır. Bu savaşta bilgiyi insan beyninde şekillendiği andan itibaren fiziki ortama taşındığı ana kadar olan süreçte iyi yöneten hep bir adım öne geçecektir. Belge/bilgi yönetimi alanının da yeni gerçeklikleri tespit edip kendisine güncel ve vizyoner bir yol haritası çizerek hızla gelişip evrilmesi gerekmektedir. Bu çerçevede bildiride geçmişten alınan bir takım örneklerden de hareket edilerek "Endüstri 4.0" ve yeni gerçekliklerin olası görünen etkileri tespit edilmeye çalışılarak, geleceğe yönelik yapay zekâ ve diğer yeni gerçekliklerden hareketle, belge/bilgi yönetimi uygulamalarının istihbarat alanındaki etkisine, bilginin bilgiyle, makinenin insanla, doğal zekânın yapay zekâ ile olan mücadelesinde hangi tarafın avantajı elinde bulundurabileceğine dair düşünceler -ve belki de temenniler- dile getirilmektedir.

Anahtar sözcükler: *Belge/Bilgi Yönetimi, Tarih, Endüstri 4.0, Yapay Zekâ, İstihbarat.*

Giriş

"Eyleme dönüşen biraz bilgi, boş duran fazla bilgiden sonsuz derecede daha değerlidir.-Halil Cibran"

19. ve 20. yüzyıllarda sanayi ürünleri çevresinde gelişen, ilerleyen insanlık günümüzde bilgi, enformasyon, iletişim teknolojileri ve ağlar üzerinden yolculuğuna devam etmektedir. Daha önceleri de tarım ekonomisinin etkisiyle

“toprağa sahip olma” denkleminde yürüyen güç kazanma mücadelesi, sanayi ekonomisinde “üretim kapasiteleri ile materyallerinin kontrolü ve ele geçirilmesi” üzerinden hareket etmiş, her alanda rekabeti, savaşmayı insanlığın önüne koymuştur.

H. G. Wells (2004, s. 78) insanlığın büyük bir değişim geçirdiğini ama bu değişimin gelişmesini takip edecek bir araca sahip olunamadığını söylerken, “Dünyamız büyük bir değişim geçiriyor. Yaşam koşullarında meydana gelen değişim, insanlık tarihi boyunca hiçbir zaman son elli yılda yaşananlar kadar hızlı ve büyük olmamıştı. Hala, olaylar zincirinin hızlı bir şekilde gelişmesini takip edebilecek bir araca sahip değiliz. Biz ancak, şu anda üzerimize doğru gelen değişim rüzgârının gücünü ve şiddetini yeni yeni anlamaya başlıyoruz.” ifadesiyle bir anlamda insanlığın şaşkınlığına da tercüman olmaktadır.

İnsanlık elbette bilinen tarihi boyunca sürekli bir değişimin içerisinde olmuştur. Ama hiçbir zaman bugünkü kadar hızlı ve dünyanın en ücra noktalarına kadar anında nüfuz edecek bir yapısallıkla karşılaşmamıştır. Geçmişte bu değişiklikler aslen içerik olarak birbirine bağlı ve bağımlı biçimde -şimdi fark ediyoruz ki- sindire sindire ortaya çıkmıştır. Ancak 21. yüzyılda mücadelenin içeriği ve araçları çok değişmiştir. “Bizim bugün, dünya genelinde kültürel olarak bulunduğumuz nokta budur. Kendimizi, bilgi kaynak ve kurumlarının denetimi için sürdürülen bir mücadeledeki ithamların çatışması içerisinde buluyoruz (Wallerstein 2013, s. 14)”. tespiti çağımızın her taraftan çatışmalarına göndermede bulunmaktadır. Bizim de gözlemlediğimiz, şahitlik ettiğimiz şudur ki, bilgi kaynaklarının ve kurumlarının denetimi mücadelesinde gelinen nokta, doktrinel anlamda bildiğimiz birçok şeyi de değiştirmiştir. Askeri doktrinler, stratejik doktrinler, savaş doktrinleri günümüzde yakın geçmişe göre çok ciddi değişikliklere uğramıştır. Bu mücadele sonucu, bilişim teknolojileri, haberleşme teknolojileri, telsiz sensör ağları, uzay teknolojileri, internet, ileri malzemeler, nanoteknoloji, biyoteknoloji, nano-solar enerji pilleri, temiz enerji, yapay zekâ, derin öğrenme, gen mühendisliği, nesnelerin interneti, sezgisel algoritmalar vd. ile ilgili çalışmalar mevcut paradigmaları altüst etmiştir. Bu çerçevede;

- Ekonomik ilkelerde, uygulamalarda değişim,
- Güvenlik kavramlarında değişim,
- Organizasyonel değişim,
- Liderlik kavramında değişim gerçekleşmiştir.

Küresel ölçekte işbirlikleri sinerjiyi artırarak küresel devasa kurumları oluşturdu. Devasa kurumlar ise küresel devasa rekabeti ortaya çıkardı. Asker-sivil, savaş-barış arasındaki ayrım bulanıklaştı, bilgi altyapısı kritik altyapı haline dönüştü, teknolojinin kolay edinimi ve kullanımı ile asimetrik tehdit riski arttı, hiyerarşiye göre değil, işleme göre organizasyon yapısı ön plana çıktı, kurumlar arası ortak, eş zamanlı bilgi erişimi ve paylaşımı sağlandı.

Günümüzdeki bu devasa değişimi en iyi anlatan kavramlardan bir tanesi, Avusturyalı iktisat profesörü Joseph Schumpeter'in 'Yaratıcı Yıkım' tespitidir ve özelinde yenilik kavramını ele alır, endüstriyel toplumun gelişmesinde kendi kendini yenileyen statik bir akım tablosu yerine dinamik bir gelişme modelini çerçevelendirir. Gelişmeyi denge çizgisinin aşılması ve yeni bir denge çizgisine yönelmek olarak tanımlar. Literatürde bu kavrama birçok gönderme yapılır. Uçkan ve Ertem (2011, s. 18) yaratıcı yıkımı şu şekilde izah ederler:

"Joseph Schumpeter'in deyimiyle 'yaratıcı yıkım' eskiyi silip yeniye yol açarak ilerliyor. Bu oyunda artık sadece devletler ve çokuluslu şirketler oynamıyor. Yeni ve davetsiz oyuncular oyuna girdi. Artık oyunda kurumsal ve endüstriyel medya düzenini bozan, bilginin dolaşımı önündeki engelleri yıkan, onların yanından dolaşarak iktidar odaklarının kirli sırlarını ifşa eden Wikileaks'in temsil ettiği yeni bilgi oyuncuları da var."

Bilgi çağı diye tanımlaştırılan günümüzün yaratıcı yıkımı ise teknolojik gelişmeler olarak nitelenebilir. Yeni ve davetsiz oyuncular artık bilgi teknolojileri endüstrisinin uzantılarıdır. Abdulkadir Çevik'in (Kış 2002, s. 216), "Her değişimde olduğu gibi, mutlaka bir bedel ödenecektir. Bu değişimin bireyler ve insanlık için getirdikleri de götürdükleri de olacaktır." teşhisi günümüzdeki yaratıcı yıkıma bir bedel ödeyeceğimiz gerçeğini bizlere hatırlatmalıdır. Hedef, ödenecek bedel karşılığında elde edileceklerimizin kaybettiklerimizden daha fazla ve yararlı olarak bize geri dönüş yapması olmalıdır. Bu da kişiselden daha çok kurumsal sorumluluklar ve eylem planlarını gerekli kılmaktadır. Dünyadaki gelişmeler zaten bu değişimin de ödenen/ödenecek bedellerin de ne olacağı ile ilgili birçok veriyi bize sunmaktadır.

Turquie diplomatique Gazetesinin Kasım 2017 sayısında (s. 1), economist.com'dan "Petrol Tekelinden Veri Tekeline mi? Dünyanın En Değerli Kaynağı Artık Petrol Değil Verilerdir" başlığıyla aktardığı makalede, veri ekonomisinin, anti-tröst kurallarına yeni bir yaklaşım gerektirdiğinden bahisle "Yeni emtia, onun akışını kontrol edenleri sınırlandırmak üzere anti-tröst düzenleyicilerinin devreye girmesine yol açacak şekilde karlı ve hızlı büyüyen bir endüstriyi ortaya çıkarıyor. Bir yüzyıl önce, söz konusu kaynak, petrolün ta kendisiydi. Şimdiyse benzer endişeler, devlet tarafından veriler –dijital çağın petrolü- alanında gündeme getiriliyor. Bu devler –Alphabet (Google'ın kardeş şirketi), Amazon, Apple, Facebook ve Microsoft- durmak bilmez gibi görünüyorlar. (…) Endişelenmek için sebep var. Internet şirketlerinin verileri kontrol etmesi, onlara devasa bir güç kazandırıyor. Rekabete dair ta petrol çağında tasarlanmış olan eski düşünme biçimleri, artık 'veri ekonomisi' olarak adlandırılan süreçte miadını doldurmuş görünüyor. Yeni bir yaklaşıma ihtiyaç var. (…) Verilerin bu kadar bol olması rekabetin doğasını da değiştiriyor. Teknoloji devleri, ağ etkilerinden her zaman faydalanmıştır. (…) Ancak, eğer hükümetler veri ekonomisine belirli sayıdaki teknoloji devinin yön vermesini

istemiyorsa, ellerini çabuk tutmaları gerekiyor." değerlendirmesini dikkatlere sunarken her seviyeden yönetim mekanizmalarına da uyarılarda bulunuyor.

Elbette istihbarat doktrininin de bu değişimlerden etkilenmemesi diye bir şey söz konusu olamazdı. Bu değişimin temelinde ağ yapılar, sanal ortamlar ve bir meta olarak bilgi mevcuttur. Kahn'ın (Yaz 2002, s. 8), "İnsanoğlu fiziksel objelerden bilgi edinmenin ilkel kapasitesine, bu bilgiyi kelimelerden de elde etme becerisini ekledi. Bu sözel beceri onu, av ya da kaçan yırtıcıların peşindeki hayvan ya da insanların kullandığı bilginin çok daha güçlü bir biçimine kavuşturdu. Bu da haber almanın bugünkü önem seviyesine yükselmene neden oldu." tespitiyle istihbaratın değişen doğasını aktarıyordu. Bu değişimin bugünkü hali olan verilerin, bilgilerin çoğalması, yığılması, endüstriyel uygulamaların konusu olması göz ardı edilecek bir unsur değildir. İnsan algılamaları üzerinden değişimler ise daha da hızlı gerçekleşmektedir.

Yeni gerçekliklerin biçimlendirdiği günümüz dünyasının en önemli öğesini teknolojik gelişim, iletişim ile ekonomi, bilgi elde edilmesi, bunun nitelikli olarak değerlendirilmesi, yerinde ve zamanında kullanılmasıyla birlikte güvenlik, dolayısıyla istihbarat arasındaki dengenin kurulması oluşturmaktadır demek mümkün hale gelmiştir. Bu dengenin kurulması noktasında ölçekler de büyük değişimlere uğramıştır. Artık devletlerin toplumların güvenliği, esenliği, huzuru bazen çok ufak gibi görünen bu nedenle önemsenmeyen, bir kişiye ait veya onun sahip olduğu ufacık bilgi kırıntısına bağlı olabilmektedir. Devlet ve toplum olarak güvenliğe ve bağımsızlığa tarihin her döneminden daha çok ihtiyacın olduğu, hissedildiği günleri yaşamaktayız.

Geçmişte savaşları yaya askerler, kılıç, kalkan, ok kullananlar, at, fil, deveye binenler, zırh giymiş yeniçeriler, şövalyeler, daha sonra ateşli silah kullananlar, toplar, tanklar, gemiler, uçaklar, kurmaylar, efsane liderler sevk ve idare etmişken günümüzdeki savaşları yüzyüze karşılaşmadan, çarpışmadan elektronik âlemlerde ağlar üzerinde hâkim olan farklı bir sınıf sevk ve idare etmektedir. Savaş kesintisiz birey birey sürmektedir. Platon'un şu sözü hayata dair bu gerçekliği en iyi biçimde yansıtır: "Yeryüzünde savaşların sona erdiğini sadece ölüler görmüştür." İnsanların bulunduğu, mücadelenin ve savaşın hem taktiksel hem de operasyonel olarak sürdüğü her kısmında istihbarat teşkilatları da yer alır.

Belgenin/Bilginin Yeni Güzergâhı Ağlar ve İstihbarat

Teknolojinin şaşırtıcı ve beklenmedik biçimlerde ilerlediğinden bahseden Graeber (2016, s. 37), bunun genel olarak ne yönde ilerleyeceğinin sosyal faktörlere bağlı olduğunu belirtir. Ancak yaşadığımız şu dünyada artık toplumlararası, vatandaşlar arası ve daha üst düzeyde küresel anlamda insanlar arası iletişim, etkileşim ağlar üzerinde yürüyüp örgütlenmektedir. Ağlar küresel yeni bir sosyal-ekonomik-kültürel-askeri (vd.) morfolojiyi ortaya koymakta ve

ağlar üzerinde yürütülen iletişim ve etkileşim eskiden farklı bir mantık geliştirerek yeni hayat formları, üretim, denetim, deneyim, yönetim, iktidar, hukuk, eğitim, kültür süreçlerinde önce kişisel, sonra sosyal ve neticede küresel düzeyde önemli yapısal değişiklikleri gerçekleştirdiği görülmektedir. Yani sosyal olguların belirlediği teknolojik ilerlemenin yönünden daha çok günümüzde teknoloji, sosyal faktörleri etkileyip yönlendirmektedir. Bugün dünya küçülmüş avuçların içine sığar olmuştur ve parmak uçlarıyla her yere erişilebilmekte, fiziki sınırların çok da koruyuculuğu kalmamaktadır.

Michael Hardt ve Antonio Negri "İmparatorluk" (2008, s. 18) adıyla ülkemizde yayımlanan kitaplarında yeni bir ağ iktidarının şekillendiğinden bahsederek küreselleşme süreçlerine paralel olarak ulus-devlet egemenliğinin, hala etkili olsa da, giderek gerilediği iddiasındadırlar. Üretim ve mübadelenin asli unsurlarının – para, teknoloji, insanlar ve metalar- ulusal sınırları daha kolay geçtiğini, dolayısıyla ulus-devletin bu akışı düzenleme gücünü ve ekonomi üzerindeki otoritesini günden güne yitirdiğini, en baskıcı ulus-devletlerin bile artık bırakın dışarıyı, kendi sınırları içinde bile üstünlüğünü ve egemen otoritesini yitirdiği tezini dile getiren yazarlar, ulus-devlet egemenliğinin gerilemesinin genel olarak egemenliğin gerilediği anlamı taşımayacağını da ekleyerek, bu yeni gerçekliğe imparatorluk adını verirler. İmparatorluk terimini çağdaş küresel düzeni adlandırmak maksadıyla, emperyalizm terimiyle karşıtlık yaratacak şekilde kullandıklarını söylerler (s.14). Emperyalizm kavramının gelinen noktada artık küresel iktidar yapılarını anlatmakta/anlamakta yeterli bir kavram olamadığı düşüncesini dile getirirler. İkili sınırların artık ortadan kalktığını söylerler.

Michael Hardt ve Antonio Negri'nin sınırların kalkması meselesine ciddi oranda itiraz edenler de bulunur. Mark G. E. Kelly (2016, s. 8) bunlardan birisidir, bu görüşe şiddetle karşı çıkarak kendi iddiasının bunun tam aksi olduğunu, sınırların kalkmak, yok olmak yerine gün geçtikçe kalınlaştığı iddiasını dile getirir. Tartışmayı Foucault'nun biyoiktidar ve biyopolitika kavramları üzerinden sürdüren Kelly (s. 20), "Küresel yönetimsellikten ziyade küresel bir biyopolitikanın söz konusu olup olmadığı sorunu, şu iki şeyin var olup olmadığı sorununa indirgenmiştir: Küresel bir nüfus ve –bunun inşası ve düzenlenmesine olanak sağlayan- küresel bir aygıt. Eğer bu ikisinin varlığından söz edilemiyorsa, yalnızca bu türden Foucaultcu bir küresel biyopolitikanın değil, aynı zamanda – geleneksel, ulusal hükümetlerle aynı düzenin bir parçası olarak düşünülebilecek- hiçbir küresel hükümetin/küresel yönetimin de esamisi okunmaz (s. 27)." ifadeleriyle düşüncesini çerçevelendirir. Küresel politikanın varlığına aykırı ilk noktanın ise devletler arasındaki sınırların varlığını halen sürdürüyor olmasıdır (s. 29), diyerek iddiasını sürdürür.

Leonard M. Dudley (1997, s.20) de, bazen devletin resmi sınırlarının yönetici grubunun fiili iktidar sınırlarıyla farklılık gösterebileceği görüşündedir. Dudley (1997, s. 34), meseleye egemen grupların gerçek yetki ve mali güç sınırları üzerinden bakar, siyasal birimin coğrafi sınırını, dış sınır, toplum içerisindeki kamu faaliyetlerini özel faaliyetlerden ayıran sınırını, iç sınır olarak ayrıma tabi

tutar. Dış sınırın, bir noktadan kontrol edilen toprakların büyüklüğünü belirlediğini söyler. İçinde yaşadığımız şu çağda güç sınırı unsurları da ömrünü tamamlamak üzeredir. Artık teknolojinin günümüzde geldiği noktada, etki alanları ağ yapılar üzerinden genişleyip farklı yapısallıklara bürünerek oluşmakta, ancak egemen olma, yönetme döngüsü şekil değiştirse de içerik olarak aynen devam etmektedir.

Ağ yapılarını elinde tutan, teknolojinin gelişimine yön veren toplumlar veya organizasyonlar, kendi ülkelerinin sınırları içerisinde kalmıyorlar. O teknolojiyi icat eden ve bunu kullanılır hale getirenlerin fiziki bir devlet sınırından bahsetmek veya yetkilerini, etkilerini kendi devletlerinin sınırları içerisinde tasavvur etmek mümkün değildir. Microsoft, Apple, Facebook, Linkedin, Twitter ve adını saymaktan yorulacağımız buna benzer oluşumları hangi dış sınırla çerçeveleyebiliriz? Toplumları, kişileri değiştirdiği, yönlendirdiği hususunda hemfikir olmayanımız var mıdır?

Yeni egemen sınıf, dünyayı avuçların içine sığdıran, önce parmak uçlarından yola çıkıp göze, kulağa sonra benliklere, kişiliklere, oluşumlara etki edip yön verenler, değiştirenler, fark ettirmeden yönetenlerdir. Küçülen, sınırsızlaşan dünya meselesinin farkına varılmasının geçmişi de öyle çok yeni değildir.

Küçülen Dünya (Shrinking World) yaklaşımı, Birinci Dünya Savaşı'nın ardından, 1929 yılında Macar yazar Karinthy tarafından ortaya atılmıştır. Aslen basit hikâyeler yazan Karinthy, bilim kurgu tarzında yazdığı 'Zincirler' (L\aancszemek) adlı hikâyesinde, 'zincir bağlantılarından' bahsederek kişilerin birbirine bağlantısını ifade etmiş ve sanılanın aksine, dünya nüfusu arttıkça aslında insanlar arasındaki bağların daha da kısaldığını ifade etmiştir. Hikâyede dünya üzerinde herhangi iki kişi arasında en fazla 6 kişi arasında bir bağ kurulabileceğini iddia etmiştir. 'Six Degrees of Separation', altı derecelik ayrım, altı derece uzak veya ayrımın altı derecesi olarak Türkçeleştirilen bu teori, Frigyes Karinthy'nin bir önermesidir. 1929 yılına göre çok büyük oranda gelişen teknoloji ve iletişim olanakları ile kişilerin çevreleri bugün daha genişlemekte ve daha çok kişiye ulaşılabilmektedir. Bu anlamda dünyanın büyüdüğü ancak aynı zamanda da küçüldüğünden ve Frigyes Karinthy'nin bu teorisinin gerçekleştiğinden bahsetmek mümkündür. Sosyal psikolog Stanley Milgram, bu teori ile ilgili olarak deneyler kurgular ve özel hesaplamalarla '6 Derecelik Ayrım Teoremi'ni akademik bir fenomene dönüştürür.

Bu teori yalnızca insanlar arasındaki uzaklığın en fazla 6 derece (kişi) olduğunu söylemez. Aynı zamanda diğer canlı, cansız ve soyut ağlar için de geçerli olduğu iddiasını taşır. Örneğin, ekonomiler, terörist oluşumlar, salgın hastalıklar (pandemi; ebola, aids gibi), modalar, trendler, reklamlar, akımlar, dedikodular, buluşlar, iş bulmalar, evlilikler, fikirler vb. hep bu 6 Derecelik Ayrım teorisi çerçevesinde işler, gelişir. Böyle bakınca bekârken evleneceğiniz kişinin en fazla 6 kişi uzakta olduğunu bilmek ilgi çekici olsa gerektir. Veya dünyanın herhangi

bir yerinde yaşayan hayalinizdeki oyuncuyla, sporcu veya siyasetçiyle tanışma ihtimalinizin ne kadar fazla olduğunu bilmek de ilginç olacaktır. Düşünsenize, tanışmak istediğiniz O kişi en fazla tanıdığınızın tanıdığının tanıdığının tanıdığının tanıdığı olacaktır.

Burada daha ilginç olan bir şey de ilk sosyal ağ sitesinin Facebook değil de, 1997 yılında yayına başlayan SixDegrees.com sitesi olduğudur. Fark edileceği gibi bu sosyal ağın ilham kaynağı yukarıda sözü edilen 6 Derecelik Ayrım (Six Degrees Separation) teorisidir. Bu site üyelerine, profil oluşturma, arkadaşlarını listeleme ve arkadaşlarının listelerini inceleme imkânı sağlamıştır. Six Degrees kendisini insanların bağlantı kurmalarına ve birbirlerine mesaj göndermelerine yardımcı olan bir araç olarak tanımlamıştır. Aynı Facebook gibi; Facebook'un sloganını hatırlayalım: Facebook tanıdıklarınla iletişim kurmanı ve hayatında olup bitenleri paylaşmanı sağlar. Milyonlarca kişiyi kendisine çekmesine rağmen SixDegrees.com 2000 yılında kapanmıştır. Sonrasında ise sosyal ağ siteleri mantar gibi patlar: Friendster (2003), Linkedin (2003), MySpace (2003), Facebook (2004), Twitter (2006) ve diğerleri. Sosyal ağlarla birlikte 7 milyar küsur milyonluk dünyada iki kişi arasındaki uzaklık bugün artık en fazla 4 kişiye inmiş durumda (konu için bkz.: Çakıroğlu, 2017).

İnsanları, toplumları etkileyen ve birbirine yaklaştıran bu fiili durumun devletin işleyişi ile birlikte elbette istihbarat faaliyetlerinin süreçlerini, işleyişini, örgüt ve insan kaynağı yapısını, uğraşlarını, sorunlarını ve sonuçlarını ciddi anlamda değiştirdiğini ifade etmek yanlış olmaz. İnsanların yaklaşmasıyla birlikte insanların sahip olduğu bilgi de birbirine yaklaşmış, kontrolsüz biçimde de el değiştirir olmuştur. Altı derecelik ayrımın farkında olan istihbarat kurumlarının bilgiyi hem ele geçirme hem de en fazla altı derecede kaybetmesi mümkün görünüyor. Sosyal ağ sitesinden yapılan bir paylaşım kişiselden devlete dair güvenliğe kadar her şeyi etkiliyor. Toplumsal olayların önceden tespit edilmesi, sosyal eğilimlerin belirlenebilmesi, gerçekleşen olaylarda geriye dönük araştırmalar yapılması, başka olay, olgularla irtibat kurulması için sosyal ağlar ve 6 Derecelik Ayrım (Six Degrees Separation) önemli bir istihbarat ortamıdır. İstihbarat örgütleri bu ortamlarda cirit atmalıdır veya atmaktadır. O zaman, bir istihbarat teşkilatı 6 Derecelik Ayrım (Six Degrees Separation)'ın hangi derecesinde yer alacaktır veya almalıdır diye bir soru yöneltsek cevabın geçerliliği, hukukiliği olabilir mi? Dereceye girmezseniz, yolunuzu kesiştirmezseniz kayıp kaçakları, olabilecekleri, gidilecek rotaları nasıl belirleyeceksiniz?

İş bu derecede de kalmayıp farklı unsurlar da hayata dâhil oluyor. Bu çerçevede günümüzü bilginin bu değişim, erişim gücüyle birlikte temsil eden ve yine işleri çetrefilleştiren bir kavramı da hız. "5N 1K'nın eskisi kadar önemli olmadığından bahseden Ali Saydam , 'Artık 2H var. Hız ve hikâye. Sağlam bir hikâyeniz olacak ve bunu en hızlı şekilde aktaracaksınız' diyor. Günümüzü özetleyen iki kelimecik içerisinden geçtiğimiz ve henüz tam anlamıyla da getirdiklerini götürdüklerini hesaplayamadığımız, maliyetini muhasebeleştiremediğimiz iletişim/bilgi çağının

gerçekliğini barındırıyor: Bir hikâye (herhangi bir malumat) ve bunun hızla elde edilip hızla dağıtılması ve hızla unutulması. Ertesi zaman diliminde yeni bir hikâye ve hız ilişkisi. Bu sarmal döngü çağımızın hayat formunu özetlemektedir (Torunlar, 2016, s. 417).” Hız da hayatları, insanları, toplumları değiştiriyor.

Mesela, hızın toplumları akışkan hale getirdiğini söylüyor Zygmunt Bauman (2015, 13-16) devamında ortaya koyduğu, “Ağların, yapıların yerini aldığı bir toplumda bu, övülmeye değer ve kendi içinde hayranlık uyandıran bir kültürel gösteridir, bu ağlara bağlanmak ve ayrılmak ile sonu olmayan bağlanış ve ayrılışlar kararlılık, bağlılık ve mensubiyetin yerini almıştır.” tespiti ile de günümüz dünyasının, sosyal hayatının ve bunun devlet iş ve işlemlerine yansımasını veriyor. Hayatımızı belirleyen bu hız kavramının etkileri ile her şey o kadar büyük bir süratle değişiyor ki ayak uydurmak için aynı şekilde hızlı hareket etmek durumundayız. Tek tek insanlar da onların oluşturduğu toplumlar, devleti oluşturan kurumlar, organizasyon ve örgütler de bu hızın peşine takılmış gidiyor. Ağlaşmış akışkan kamu elektronikleşen dünya ile beraber her yanımızı sarıp sarmalıyor.

“Tüm dünyada insanlardan devlet örgütlerine kadar çok geniş bir yelpazede herkes ve her kurum bu ağın kapsama alanındadır ve hizmet alımından hizmet sunumuna, elektronik dünyaya, akıllı yazılım ve cihazlara, elektronik/dijital ağlara bel bağlamıştır. İfade edilenlerin, yorumlananların çoğunun aksine, bu elektronikleşmiş dünyanın gelecekte insanlığa neler getireceği çok belirgin değildir. danah boyd günümüz insanının yaşam alanını ‘ağlaşmış kamu’ olarak tanımlar. Bu çerçevede elektroniğe dayanan teknolojiler ve sistemlerden oluşan bir yapı ile insanlar birbirine bağlıdır. İnsanlar bu ağlar veya sistemler üzerinden birbiriyle ilişki kuruyor, işlerini yürütüp, görevlerini yerine getiriyor, eylemlerde bulunuyorlar. Bu ağlar üzerindeki eylemleri neticesi, yine ağ üzerinde bir takım gruplaşmalar oluşturarak sosyalleşme veya toplumsallaşma pratiklerini gerçekleştiriyorlar. Ağlaşmış kamunun bugün geldiği noktada her şey o kadar birbirine girmiş, yeni eskiyi parçalamıştır ki, ‘mutlak gerçek (hakikaten gerçek)’ ile ‘sanal gerçek’ arasındaki ayrım çizgisi belirginliğini yitirmiştir (Torunlar, 2016, s. 424).” Aşağıda verilen örnek (burada insanlara olumlu yönü yansısa da) ağlar üzerinden hayatımıza yapılabilecek müdahaleler konusunda tüylerimizi diken diken edebilir.

‘Tesla Kasırgadan Önce Florida'daki Araçlarının Bataryalarını Arttırdı!’ (Erdal, 2017) başlıklı haber, dünyamızın ağlar, uzaktan erişimler noktasında hangi seviyeye geldiğini, biraz ürküterek de olsa bize anlatıyor:

“Tesla, Irma Kasırgasından önce bölgedeki kendi araçlarına batarya güncellemesi yaptı. Bu sayede Tesla, Florida’daki araçların bataryalarının bir süreliğine daha uzun gitmesini sağlayacak.

Tesla Irma kasırgası sırasında kendi müşterilerinin acil durumlara karşı ekstra batarya süresi için Florida'daki müşterilerine bir güncelleme gönderdi. Bu

güncellemeyle birlikte normal 60 kWh'lık bataryaya sahip araçlar 75 kWh güce yükseltildi. Hem de sadece basit bir güncelleme sayesinde. Peki, hiç bir doğrudan işlem yapılmadan araçların batarya kapasiteleri nasıl güncellendi?

Tesla Yerinde Durmuyor: Araç Sahiplerine Tercihlerine Her Yerden Erişim Kolaylığı sağlıyor. Aslında olay şu; Tesla'nın Florida'da yaygın olarak kullanılan Model S ve Model X arabaları var. İki modelinde hem 75 kWh'lık hem de 60 kWh'lık seçenekleri bulunuyor. Fiyat olarak daha ucuz olan 60 kWh'lık arabalarda ise garip olan zaten 75 kWh'lık bataryayı kullanması. Yani Tesla daha düşük özellikli sattığı modele üst modelle aynı donanımı koyuyor ancak özelliklerini yazılım aracılığıyla düşürüyor.

Bu yazılımsal müdahale sayesinde de aracını 60 kWh'lık ucuz modelde alanlar daha sonra arabalarını para karşılığı tabiri caizse " güncelleyebiliyorlar". Ya da bu tip acil durumlar olduğunda Tesla merkezden güncelleme yaparak müşterilerine böyle bedava opsiyonlarda sunabiliyor." Bugün uzaktan erişim ile menzilinizi uzatan sistemler yarınlarda başka olumsuz şeylere sebep olmazlar mı? diye sorgulamadan geçmemek lazım.

Ağ yapılar, içerisinde yaşadığımız için çok farkında olmasak da buna benzer öyle köklü değişimleri hayatımıza dâhil etmiştir ki çok yakın geçmişe ait şeyleri bile unutarak sanki çok eskide kalan şeylermiş gibi davranmaya başladık. Bu çerçevede geçmişte istihbarat faaliyetlerine ait araçlar, yöntemler (bugün de belirli bir düzeyde önemini korumakla, ancak giderek kullanımdan el etek çekerek kaybolmakla beraber) de ciddi değişikliğe uğramıştır. Kemal Koçer'in (2003, ss.93-94) 'Kurtuluş Savaşında M. M. Örgütünün Gizli Eylemleri' adıyla kitaplaştırdığı anılarında bahsettiği casusluk hikâyeleri ve bunları gerçekleştirirken kullandıkları materyaller bugün için nostaljik yansımalardan ibaret kalmış gibidir: "Grup'ta güçlü haber alma çalışanları vardı. Pek olanaklı bir fotoğraf makinesi, kimi belgelerin fotoğrafını almakla, dil bilen bir arkadaş çeviriyle uğraşıyordu. (…) Belge taşınmasında ve korunmasında Türk kadınlarından da yararlanılmıştı. Şükufe Nihal'le kardeşi Muhsinenin hizmetleri olmuştu. Durumuyla dikkat çekmeyen evimdeki hizmetçi kızın, çok zamanlar belge taşıdığını ve aldığı görevinin önemini anlayabilecek yüksek karakterde olduğunu belirtmeliyim." Halen bu anlatılanlara benzer olaylar yaşanmakla birlikte artık sahada çalışan insan unsuru da dâhil olmak üzere birçok materyal yerini ileri düzeyde gelişmiş teknolojiye bırakır gibi gözükmektedir. Belgeler elektronik âlemde, elde etmeler, göndermeler ağ yapılarda, saklamalar bulut teknolojisinde diye listeyi uzatmak mümkündür. İstihbaratın doğası, ekolojisi, niteliği, içeriği, yapısı değişmiştir. Bu değişimin ilk başlangıç noktalarında bugün çok ilkel göreceğimiz teknolojilerin o dönemlerde dünyayı şaşkınlığa uğrattığını söyleyen Ergun Hiçyılmaz'ın (2008, s. 7), "Casus uçakları U2'ler gündeme geldiğinde dünya şaşkına dönmüştü. Oysa şimdi uzaydan görebilen, duyan bir sistem var. Teknoloji bilgisayar sistemini en üst noktaya çıkardığında, dinleme mesele olmaktan uzaklaştı ve binlerce kulak harekete geçti." karşılaştırmasında

söz ettiği uzay teknolojisinin ürünlerinin bile modasının geçmekte olduğunun ilan edileceği günler de yakın gibidir.

Bu yapısal değişim edebiyat alanına da nüfuz etmiştir, artık istihbarat faaliyetlerinin ana tema olarak alındığı birçok romanda olaylar ağ yapılar üzerinden temellendiriliyor. Geçmişte klasik belgeler ve materyallerin casusluk işlerinde kullanıldığı roman örgülerine artık sanal ortamlar, ağlar, teknolojiler, uzaktan erişimler, yönlendirmeler temel oluşturmaktadır. Örneğin İngiliz yazar Jonathan Holt tarafından üçleme olarak kaleme alınan 'Yüz Karası, Kayıp Geçmiş ve Hain [Yapı Kredi Yayınları]' adlı romanlarda olayın önemli bir kısmı ana karakterlerden biri olan gizemli bir bilgisayar dâhisinin yazılımını yaparak kullanıma sunduğu Carnivia adlı bir sosyal paylaşım sitesi üzerinde gerçekleşmektedir. Bilgisayar dâhisi bu karakter, devlete kurguladığı siteye erişim izni vermediği için de yargılanmaktadır. Bu sitede insanlar birçok gizli bilgileri ve sırları paylaşmaktadır. Olayların çözümü bu paylaşımlar kullanılarak, sanal ortamlar dolaşılarak sağlanır. Romanda işlenen bu husus, kişisel bilginin korunması ile devletin güvenliği arasındaki çatışmaları açığa çıkartmayla ilgili modern tehditleri içeren gerçeklikleri gözler önüne sermektedir. Olay örgüsü içerisinde ABD arşivlerinden Vatikan arşivlerine ve oradan da sanal âlemlere uzanan tarihsel perspektif içerisinde devletin güvenlik ihtiyacı ve hassasiyetlerinin nasıl değiştiğini de izlemek mümkündür. Bu noktada modern çağın önemli ve sık sorulan sorusu devreye girmektedir. Devlet güvenliğini nelere rağmen, nasıl sağlayacağız? Bunu yaparken nelerden fedakârlıklarda bulunacağız?

Yeni Gerçekliklerin Yansımaları: Hissettirmeden Yönetmenin/Yönlendirmenin Teknik Adımları, Teknoloji-Belge/Bilgi Yönetimi, Endüstri 4.0-Yapay Zekâ

Tarihte köle ticareti, ülkelerin işgali, kaynaklara el konulması, ticaretin tek taraflı yürütülmesi gibi metotlarla sömürüyü cisimleştirenler, günümüz koşullarında uzaktan erişim, yönetim teknikleriyle insanları, toplumları kendilerine, ülkelerine, kültürlerine, tarihlerine, değerlerine yabancılaştırıyor ve sahip oldukları zenginlikler farkında olunmadan birer birer ellerinden alınıyor. Bu konuyu çok detaylandırmasak da öncelikle sömürgeciliğin amacına ve yöntemine açıklık getirmek lazımdır. Jean Gottmann'ın (2003, ss. 205-206), konuyu özetleyecek şu ifadelerine bakalım: "Sömürge savaşları, kıta savaşlarından oldukça farklıdır: Düşmanın imha edilmesi değil, fethedilen halkın ve toprakların belli bir kontrol altında organize edilmesini amaçlanır. (…) Sorun 'düşmanı' kesin yenilgiye uğratmak değil, pahalıya mal olmayacak şekilde hâkimiyet altına almaktır. Bu amaçlar çerçevesinde, sömürge savaşları ele geçirilen toprakların işgal altında tutulmasını ve organizasyonunu gerektirir. Bunlar birbirine bağlıdır. Çünkü başarılı bir işgal başarılı bir organizasyona bağlıdır." Geçmişteki sömürgeciliği

tahlil eden bu ifadelerle varılan sonuç günümüz dünyası için de geçerlidir. Bir tek farkla: Geçmişte sömürgeciliği getiren işgal ve organizasyon ikilemesi görünürlüğünü yitirmiş, sanal ortamlara, ağ yapılara, internete gizlenmiştir. Tarihte sömürgecilik herhangi bir devlet-millet için toprağın ele geçirilmesi gibi coğrafi ve fiziki eylemleri şart koşarken, günümüzde bunlarla birlikte zaman/mekân mefhumunu da ortadan kaldırarak birey birey herkesi neticede küresel tüm insanlığı başarılı bir organize yapısallık ile işgal edip yönlendirilmeye, sömürülmeye aday hale getirmektedir. Bugün teknolojik yenilikler, iletişim teknolojisi, nesnelerin interneti ve yapay zekâ çalışmaları sömürgeleştirmenin teknik adımlarla ilerlemesi olarak kendisine yol çizmiştir ve ilerlemeye devam etmektedir. Feenberg'e (2010, s.25) göre "teknoloji azınlığın çoğunluk üzerindeki hâkimiyetini yeniden-üretecek şekilde yapılandırılabilir, yapılandırılmıştır da. Bu tek yönlü bir sebep sonuç oluşturan teknik faaliyetin bizzat yapısına yazılmış olan bir imkândır."

İletişim/enformasyon veya endüstri 4.0 çağı kavramlarının zihnimizde oluşturduğu çağrışımlar hep olumlanarak resmedilmektedir, ancak bu kavramların uygulama karşılığı kullanıcı olarak bizi içerikle beraber farkındalık oluşturmadan yeni hayat tarzlarına yönlendirir ki bu da teknolojinin arka yüzünü/planını oluşturur. Bu arka planın gerçekleştirmek istedikleri, teknolojinin iddia edilen ve genel kabul gören hayatımıza kattığı güzellikler, kolaylıklar, kazandırdığı söylenen özgürlükler söylemlerinden daha önemlidir. Bu hususta bilinmeyenler bilinen ve yaşananlardan çok fazlasını kapsar

Eğer bu kavramların içeriğini kendi değer dünyanızın gerçeklikleri ile doldurabilirseniz, teknolojinin arka planı ile kişinizi, toplumunuzu örtüştürebilirseniz kimliğinizi korumuş, geliştirmiş olursunuz. Ancak size sunulanı değerleriyle birlikte ithal edip sorgulayıp süzmeden bünyenize aldıysanız zaman içerisinde kimliğinizin, yerelliğinizin erimesinden, mutant olmaktan kurtulamazsınız. Bu hayatın her safhası için geçerlidir ve tarih tekerrür etmektedir, sızma ve değişim hareketi geçmişte olduğu gibi yoğunluklu olarak öncelikle ekonomik yapısallıkla birlikte başlatılmış gibidir.

Dünyanın bugün geldiği noktada sömürgecilik veya yayılmacılık kavramları modernizme, bilgi/iletişim/enformasyon çağına ve entelektüel iklime uymuyormuş gibi görünmekle beraber, gelişen birey, onların hakları, güçlenen sivil toplum gibi sunum ve propagandalarla Avrupa merkezli değerler sistemi, teknolojinin bilgi toplumu, bilgi ekonomisi vb. etiketleriyle hayatlarımızı formatlıyor. 18., 19. ve 20. yüzyılın Avrupa merkezciliği yeni sürümleriyle son hızla hayatiyetini devam ettirirken, farklı uluslararası güç mücadelelerinin aktörleri de kurgusal yönlendirmelerine, çatıştırma faaliyetlerine devam ediyor. Bu anlamda bilginin yönlendirme maksatlı kullanılması, teknolojik ilerlemelerin arka planının açık edilmesi zorunluluğu doğuyor.

"Teknolojik gelişmelerin yönünü ve niteliğini belirleyememek, bize sunulanların ötesinde yazılımlarda, ağ yapılarında olabilecek gizli geri plan ajandalarını

bilememek, tespit edememek sıklıkla elektronik/dijital dünyanın nimetlerini veya külfetlerini yanlış anlamlandırmalara, adlandırmalara, ortaya çıkabilecek kişisel, kurumsal, devletsel güvenlik açıklarını tanımlayamamaya, bu risklere ya gereğinden fazla misillemede bulunup tepki vermeye veya hiçbir şekilde karşılık vermemeye sebep olmaktadır. İsrailli istihbaratçı Efraim Halevy, soğuk savaş döneminde bilginin, yeterli verinin olmaması veya bunların yanlış yorumlanmasının barındırdığı tehlikelere dikkat çeker: 'Yaşamla ölüm arasındaki keskin çizgi olan bilgi, hiç olmadığı kadar rağbet görüyordu ve müttefikler arasında bilgi paylaşımı, ortak kaderin hayati bir parçasıydı. Bilginin olmaması veya yanlış yorumlanması, kelimenin tam anlamıyla ulusal bir felakete yol açabilirdi.' Bugünkü dünyada malumatların yanlış yorumlanması, eksik, uydurulmuş, yönlendirmeli bilgi nelerimize mal olmaktadır? (Torunlar, 2016, s.427)."

05 Kasım 2017 tarihli Hürriyet Gazetesi'nde (s.10) yayımlanan '200 dolara sokak çatışması' başlıklı bir köşe yazısında toplumların, toplulukların farkında olmadan, uzaktan erişim ve yönlendirme ile nasıl bir çatışma ortamına sürüklenecekleri gözler önüne seriliyor. Selçuk Şirin tarafından kaleme alınan köşe yazısında, ABD'de Rusya tarafından kontrol edilen 'Heart of Texas' adlı Facebook hesabından önce Teksas'ta oturanlar 'Teksas'ın İslamizasyonuna son' denilerek 21 Mayıs 2016 günü Müslümanlara ait bir kültür merkezinin önünde protesto eylemine davet edilirler. Aynı gün, aynı Rusya kaynaklı hesap bu sefer 'United Muslims of Amerika' (Amerika'nın Birleşmiş Müslümanları) adlı bir hesabı kullanarak bu sefer de Müslümanlar lehine bir eylem çağrısı yapar. 'İslami düşünceyi koruyalım' başlıklı bu çağrıda da Austin bölgesinde oturan herkes, aynı İslami kültür merkezinin önüne davet edilir. 21 Mayıs geldiğinde tüm kameraların önünde Rusya tarafından oraya yönlendirildiklerinden habersiz iki grup birbiriyle kavgaya tutuşur. Sonuç tam bir toplumsal çatışma, dinler arası kinin, nefretin artışıdır. Dünyaya da bu mesaj naklen verilir. Orada çatışan hiç kimse sahnenin arkasında, 200 dolarlık bütçeyle oluşturulmuş bir Rus sosyal medya hesabının olduğunu bilmez. Teksas örneği bize, toplumsal bir ayrışım noktası ile birlikte ucuz ve kolay erişilebilir bir teknolojinin birlikte kullanılması ile bırakınız devletler arası küçükten büyüğe gruplar arası, kimlikler arası, etnik unsurlar arası bir çatışma çıkartılıp bundan ciddi bir kaos doğurulabileceğinin ne kadar kolay olduğunu gösteriyor.

Teknolojinin nimetleri daha da çeşitleneceğine, bundan geriye dönüş olmayacağına göre yapılacak şey, yenidünya gerçekliklerine ayak uydurmak ve teknolojik gelişimde icad eden olmakla birlikte, kullanımı noktasında da iradeyi elde tutabilmektir. Bu noktadan hareket ettiğimizde, sömürgeciliğin, sızma hareketinin, yönlendirilmenin, yönetilmenin, istikrarsızlaştırmanın teknolojik adımları istihbarat teşkilatlarının da doğrudan çekim alanına girer. Ama her şeyin olduğu gibi istihbarat-teknoloji birlikteliğinin de iki yüzü vardır:

Teknolojinin dünyayı ve tek tek bireyleri getirdiği noktada *istihbarat yapmak daha kolay* gibi görünmekle birlikte aynı oranda *istihbaratı kaybetmek de daha*

kolay hale gelmiştir. ABD Anti-Terör Dairesi Eski Başkanı ve 2010 yılında bestseller olan 'Cyber War' (Siber Savaş) kitabının yazarı olan Richard A. Clarke, bu tezimizi doğrulayan açıklamalarda bulunarak istihbaratın, casusluğun eskiden zor olduğunu söylüyor (Tanış, 2012, s. 2), " 'Eskiden Washington'daki Rus Elçiliği'nde çalışan bir KGB ajanının bir FBI ajanını ayartması çok zordu. Ama şimdi Moskova'da oturuyorsun. Hiçbir risk olmadan binlerce sayfa çalabiliyorsun. Eskinin casuslarına artık gerek yok.' İstihbarat örgütleri sadece insan kaynağı açısından değişmedi Clark'e göre. Altyapı'da olduğu gibi farklılaştı: 'Eskiden Sinop'ta büyük bir kulemiz vardı. Rusya'daki konuşmaları dinliyorduk. Ama şimdi buna ihtiyaç yok. Kimse radyofrekansı kullanmıyor. Ulusal Güvenlik Ajansı'nın (NSA) Maryland'deki kampüsünden bütün dünyadaki internet trafiğini izliyoruz. (…) Amerikalı asker Sinop'a gitmesine gerek kalmadan her işini masasından halledebiliyor.'"

Belgeyi/bilgiyi kontrol altında tutmak için teknolojik, idari, hukuki, kültürel birçok bileşeni bir araya getirip, hiçbir şeyi birbirine karıştırmadan, işleri Arapsaçına döndürmeden yönetmek gerekmektedir. Bu noktada ABD Anti-Terör Dairesi Eski Başkanı Richard A. Clarke'ın (Tanış, 2012, s. 2), 'kale yerine tacı korumak' önerisini şekillendirmemiz gerekiyor. Clarke, tacı korumayı, en çok korkulan, hack edilebilecek, çalınabilecek malzemenin seçilip ona odaklanılması olarak açıklıyor. Bu maksatla artık belge/bilgi yönetimine bir ürün olarak bakmaktan vazgeçmek ve bunun bir sistem ve süreçler bütünü olduğunu anlamak, hepimizi geçmişten bugüne getiren süreçleri de hızlıca sisteme aktarmak ve en çok endişe duyduğumuz belgeleri/bilgileri sistemli bir şekilde üst düzeyde korumaya almak gerekiyor.

Modern çağın temellerinin atılmasına sebep olarak görülen Avrupa'da ortaya çıkan sanayi devrimi, ya da diğer adıyla endüstri devrimi, İngiltere'de 1763'te James Watt'ın buhar gücüyle çalışan makineyi icat etmesiyle başlamış olarak kabul edilir ve yeni buluşlarla birlikte buhar gücünün yerini makineleşmiş endüstrinin alması sonucunda ortaya çıkan gelişmelerle birlikte sermaye birikiminin artışını ifade eder. Bu döneme ilk sanayi devrimi (1,0) denilir, su ve buhar gücü kullanılarak mekanik üretim sistemleri ile ortaya çıkmıştır. İkinci sanayi devrimi (2,0)'n de ise elektrik gücünün yardımıyla seri üretim başlamıştır. Üçüncü sanayi devriminde (3,0) elektronik materyallerin kullanımı dijitalleşme ve BT (Bilgi Teknolojileri)'nin gelişimiyle üretim daha geniş çaplı otomatikleşmiştir. "Asıl devrim ise, enformasyon teknolojileri – telekomünikasyon, uydu, bilgisayar, internet, veri, yazılımı, vb.- arasındaki ortaklıktan doğmuştur. Artık yerküre, bir yandan sürekli olarak uydularla gözetlenirken, diğer yandan da bilgisayarlar yoluyla elde edilen enformasyon ayrıştırma, sınıflandırma ve anlamlandırmaya tabi tutulmuştur. Böylece işin içine 'yapay zekâ' girmiş, insanlara/kurumlara ve devletlere ait her türlü bilgi artık sır olmaktan çıkmıştır. (…) Enformatik gözetimin dünyası, giderek 'çok daha renkli, daha heyecanlı, daha güçlü, daha az bilinen, daha korkutucu, daha bilimsel ve daha tehlikeli' hale gelmiştir (Dolgun, 2015, s.143.)."

Enformatik gözetim dünyasının dayandığı bu noktaya bugünlerde dördüncü sanayi devrimi (4,0) denilmektedir. Endüstri 4,0, teknolojilerin ve değer zinciri organizasyonları kavramlarının kolektif bir bütünüdür. Siber-fiziksel sistemlerin kavramına, nesnelerin ve hizmetlerin internetine dayalıdır. Endüstri 4,0'ün akıllı fabrikaların hayata geçirilmesine çok büyük katkı sağladığı düşünülmekte ve genel olarak aşağıdaki üç yapı içerisinde değerlendirilmektedir.

1. Nesnelerin İnterneti
2. Hizmetlerin İnterneti
3. Siber-Fiziksel Sistemler

Endüstri 4,0 ile hayata geçirilen akıllı fabrikalar kapsamında, fiziksel işlemleri siber-fiziksel sistemlerle izlemenin, fiziksel dünyanın sanal bir kopyasını oluşturup gerçeğe çok yakın simülasyonlar yapmanın ve merkezi olmayan kararların verilmesini sağlamanın mümkün olabileceği düşünülmektedir. Nesnelerin interneti ile ise siber-fiziksel sistemlerin birbirleriyle ve insanlarla gerçek zamanlı olarak iletişime geçip işbirliği içinde çalışabilecekleri iddia edilmektedir. Hizmetlerin interneti ile hem iç hem de çapraz örgütsel hizmetler sunulması ve değer zincirinin kullanıcıları tarafından değerlendirilmesi hedeflenmektedir.

2000'lerden sonra hayatımızın her alanına giren, elektronikleşen, dijitalleşen, sanallaşan yenidünya gerçekliliği özellikle orta yaş kuşağını klasik kâğıt üzerinde belgelendirme, buna bağlı okur-yazarlık ile elektronik ortamda üretilmiş veya o ortama taşınmış Elektronik/Dijital Evren ve bu evrenin gerçeklikleri arasında boşlukta asılı bırakmıştır. Bu sanallaşan elektronik dünya insanların düşüncelerini, alışkanlıklarını, hal ve hareketlerini, toplumsal, siyasal, ekonomik hatta askeri örgütlenme biçimlerini yeniden formatlayıp yerelden küresele doğru genleştirip genişleterek fiziksel ve zihinsel düşünce yapısını değiştirmektedir. Orta yaş kuşağı bu konuda çoğunlukla huzursuz ve endişeli iken, genç kuşak bu teknolojiyle yatıp kalkmaktadır. Bu davranışlardan doğru olanı hangisidir?

İçinde bulunduğumuz durumları, açmazları, sıkıntıları sırf teknolojiyi kullanarak, kullanıcı kalarak çözümleyip düzeltemeyiz. Teknoloji ile bireyin, toplumun ve kamunun ilişkisini, kendimizce şekillendirilecek ve kaynağını geçmiş deneyimlerimizden alacak değerler sistemi üzerinde inşa ederek sağlıklı bir güzergâha koyabiliriz. Olayın teknolojik boyutu kadar psikolojik boyutu da vardır. 'Dünyadan uzak kalmayayım, ben anlamıyorum ama yeniliklere intibak ediyormuş gibi yapayım' gibi teknolojik insan tipolojisine geçememiş ancak geçmişin de hızla eskidiğini gören ve yaşayan bir orta yaş kuşağı ile 'teknolojiyi kutsallaştırmış ve hayatının her alanını ona açmış, ona bağlamış olan genç kuşak arasındaki bu 'kuşak çatışması' yine teknolojiyi emperyal emelleri için kullananların işine yarayacaktır. Bu yalnız bizim toplumumuza, insanımıza ait bir sıkıntı değildir, dünyadaki her bireyin, her toplumun ve de hayata dair her alanın mevzusudur.

Tekin Dereli, Roger Penrose'a ait "Kralın Yeni Aklı" adlı kitabın (2015, ss. 14-15) Sunuş kısmında 20. yüzyılda gelişen teknik olanakların bilimsel görüş ve yöntemlerde de yeni yönelimlere yol açtığını ifade eder: "Bilimsel yaklaşımın temelinde yer alan doğa gözlemlerinde bugüne dek hep insan algıları esas alınmıştı. Mikroskop gibi, teleskop gibi, ya da güncel bir örnek olması bakımından, Mars'a indirilen uzay aracı gibi detektörlerin yapımında güdülen amaç, insan algılarının erimini doğal sınırlarının ötesine ulaştırmaktadır. Sonuçta doğa gözlemi denen şey, insanın dokunarak, duyarak, görerek olguları bilinç alanına (yani zihnine) aktarmasından ibarettir. Sonrası bu verileri akılla işleyerek mantıksal çıkarımlarda sonuca ulaşmaktır. Öte yandan, çağdaş algılayıcılar giderek artan oranlarda bilgisayar teknolojisinden yararlanmaktalar. (…) Artık, bir fizik modelini sınamak için doğada gözlem yapmak veya laboratuvarda deney yapmak kadar bilgisayarda benzetişim (simülasyon) yapmak da geçerli kabul edilir bir yöntem olmuştur. Yıldızları gerçekte patlatamayız veya varlıklarının kanıtları dolaylı olarak gelen karadeliklerden iki tane bulup, üstelik bir de bunları çarpıştıramayız. Ancak tüm bu olaylar bilgisayar benzetişimiyle incelenebilir."

Yarım asra yakın süredir gerçekleştirilmeye çalışılan yapay zekâ, son yıllarda dünya gündemine iyice yerleşen büyük veri (big data), yeni yöntemler, algoritmalar gibi kavram ve uygulamalarla daha önce hayal etmesi bile zor olan bir noktaya geldi. "Çoğu kez kısaca AI (Artificial Intelligence) olarak anılan Yapay Zekâ son yılların en çok ilgi çeken konusudur. YZ'nın amaçları, makineler, normalde elektronik makineler, aracılığıyla insanın ussal etkinliğini olabildiğince taklit etmek ve belki sonuçta insanın ussal etkinlik yeteneğini geliştirmektir (Penrose, 2015, s. 35)."

"Yapay zekâ terimi ilk olarak 1956 yılında John McCarthy tarafından 'akıllı cihazlar yapma konusundaki bilim ve mühendislik' olarak tanımlanmış olsa da aslında mitolojiye kadar dayanan bir hayal gücünün ürünüdür. Mitolojik dönemlerde geçen hikâyelerden Hephaestus'un altın robotları ve yaptığı heykelin canlanmasını ele alan Pygmalion'un Galata hikâyesi içerisinde hep yapay zekâ barındırmaktadır (Aksu, Candan, Çankaya, 2011, s. 137)." Mitolojik hikâyelerden günümüze birçok adım atılmış ve hikâyenin tamamlanmasına az bir süre kalmış gibi görünmektedir.

"Satranç oynayan bilgisayarlar 'zeki davranış' olarak nitelenebilecek bir davranış sergileyen makinelerin belki en iyi örneğidir. Gerçekte bu makineler bugünlerde (1989'da) 'Uluslararası Usta' düzeyinde performans göstermektedir. (…) Satranç oynayan makineler, doğru hesaplama gücünün yanı sıra 'kitap bilgisi'ne de büyük ölçüde bağımlıdır. Kabul etmek gerekirse, özellikle çabuk hamle yapılmasının gerekli olduğu durumlarda bu makineler insan satrançççıya kıyasla genelde daha iyi performans göstermektedir. Çünkü bilgisayarın kuralları, kesin ve hızlı hesaplama esasına göre alınırken, insan satranççı 'karar verme'nin avantajından yararlanmak yoluna gider ki bu işlem yavaş ve bilinçli bir değerlendirme yapmak demektir. İnsan yargıları, hesaplamanın her aşamasında, analizle gerçekleşebilenden daha fazla derinliğine dikkate alınması ciddi olasılıkların

sayısını önemli ölçüde azaltırken makine, karar vermek kaygısı olmaksızın olasılıkları hızla hesaplar ve doğrudan elimine eder (Penrose, 2015, s. 37)." tespitleri bile kısa dönemde bir hayli eskidi, çünkü sentetik konuşma, görüntü işleme, ses tanıma, bağımsız öğrenme, karar verme ve mantık yürütme kabiliyetleri artık hayatımızda yer almakta ve bu da kritik düzeyde denilebilecek bir noktada. Yapay zekânın sundukları ve bundan sonra sunacaklarının birçok sektörde dönüşüm yaratması kaçınılmaz görünüyor. İstihbarat servislerinin bundan uzak durması düşünülemezdi ve öyle de olmuştur.

"Gerçek hayatta ise, araştırmacılar beyin-bilgisayar arayüzü üzerinde çalışıyor. (…) Bu arada İsrail istihbarat servisi Mossad, 'çığır açacak' teknolojiler geliştirip kullanmak için yatırıma başlıyor. Bu amaçla Mossad, Libertad adıyla bir yatırım fonu oluşturdu. Fon, robotlar, enerji, şifreleme, kişilik fişleme, metin analizi gibi alanlarda en son teknolojileri geliştiren şirketlere yatırım yapacak (Lee, 2017, s.1)."

Bilginin işlenmesini hızlandırmak, analiz ve sentez yapmak, karar verme süreçlerini etkilemek ve iş ve işlem ilişkilerinin devamlılığını sağlamak yapay zekânın diğer kullanım alanları arasında ifade ediliyor. Teknolojinin geldiği noktada bireyler veya toplumlar olarak meseleye yalnızca bir mühendislik alanı üzerinden bakmamak gerekiyor. Mühendislik alanından belki daha da etkili ve insanlık tarihini yönlendirecek şey, bilgiyi yapay zekâlara yüklemek olacak. Yapay zekâya kodlar, algoritmalar üzerinden hangi bilgileri yükleyeceğiz, onların bunu geliştirecek yapısallıklarını hangi güzergâha oturtacağız? Yapay zekâlar kodlarını ve algoritmalarını kendileri oluşturmaya başladıklarında gelişim çizgileri hangi yönde olacak? Toplum, kurum kuruluş olarak bizler bu konuda ne kadar hazırlıklıyız, kodlayacağımız, algoritma geliştireceğimiz, yükleyeceğimiz bilgi varlıklarımız ve bilgilerimiz ne kadar düzgün, bilinebilir ve yönetilebilir? Bu sorulara cevaplarımızın hazır olduğunu söyleyebilecek bir noktada değiliz ve bu arada yapay zekânın tehlikelerine de dikkat çeken, alanında çok meşhur kişiler mevcut.

"SpaceX ve Tesla gibi dev teknoloji şirketlerinin sahibi işadamı Elon Musk Yapay Zekâ'nın Kuzey Kore'den çok daha büyük bir tehdit olduğunu söyledi. Yapay zekâ konusundaki uluslararası yarışa dikkat çeken Musk bunun Üçüncü Dünya Savaşı'nın en muhtemel tetikleyicisi olabileceğini yazdı (Musk, 2017, s.1)."

"Yapay Zekâ, insan güvenliğiyle ilgili bir dizi soruna gerçek zamanlı, maliyet etkin ve etkili yanıtlar verilmesinin potansiyel yollarından birisidir. Yapay Zekâ'nın araştırma, sınıflandırma ve yeni modellerinin tespit edilmesine dair uygulamaları, farklı kaynaklardan anlam ve içeriğin ilişkilendirilip ortaya çıkarılmasına yardımcı olabilir. (…) Yapay Zekâ insanların yetkilerini elinden aldığı gibi onları güçlendirir de. Dolayısıyla, Yapay Zekâ sistemlerinin kurulumu ve konuşlandırılmasını yönlendirmek için etik ilkelerin kullanılması gerekir. İnsan güvenliği, çok sınırlı sayıda bir elit kesim için değildir. (…) Bununla

birlikte, Yapay Zekâ'nın her derde deva olmadığını da belirtmek gerekiyor. (…) Kısacası, insan güvenliğini mümkün kılan Yapay Zekâ, doğası gereği, insanların güvensizliğini azaltmalı, insanları daha fazla güçlendirmeli ve mümkün olduğunca eşitlikçi, saydam ve hesap verebilir olmalı. Dolayısıyla, iyi politika, düzenleme ve hesap verebilirlik önlemlerinin uygulamaya konulması gerekiyor (Roof, 2017, ss. 10-11)."

Heather M. Roof'un bu iyimser temennileri gerçekleri yansıtır mı bilinmez ama geçmişteki uygulamalara baktığımızda hiçbir devlet veya topluluğun kendisine güç kazandıracak uygulamaları tüm insanlığın önüne sırf iyilik olsun diye sermediği tecrübelerle hem de kanlı tecrübelerle sabittir. Yenidünya gerçekliklerinde de bunun geçmişten bir farkının olmayacağının emareleri zaten görülüyor. Ufacık bir örnek verelim ki buna benzer binlerce uygulama verilebilir: "GCHQ (İngiltere Hükümet İletişim Merkezi)'nun 360 derece tam spektrumlu toplu derleme veri sistemi, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesini utanmaz ve küstah bir şekilde yok sayarak inşa edildi. Cihazın kayıtta olup olmamasından bağımsız olarak yapılan her telefon görüşmesi, her görüntü, girilen her website, tıbbi ve finansal kayıtlar dâhil tüm kişisel veriler, temaslar, size özel her şey artık özel değil (Vanbergen, 2017, s. 3)." Size ait her şeyin kamusala taşınması ayrı bir problem iken bir de bir başka ülke, devlet tarafından kayıt altına alınmak ciddi bir endişe kaynağı olmalı hepimiz için. Yapay zekâya sahip ürünlerin daha ne kadar özelimize gireceği de ayrı bir muamma. Bu işin içerisinde olanlar konuyla ilgili ciddi uyarılarda bulunuyorlar:

"Yazılım devi Microsoft'un kurucusu Bill Gates, insanların yapay zekânın yarattığı tehditten kaygı duyması gerektiğini söyledi. Gates yapay zekânın kontrol edilemeyecek kadar büyümesinden endişe etmeyen insanları anlayamadığını belirtti" (Gates, 2015).

"(Stephen) Hawking, 2014 yılı sonlarında "Yapay zekânın geliştirilmesi insanlığın sonunu getirebilir" demişti. Hawking'e göre yapay zekâ, kendisini her geçen gün artan bir oranda yeniden tasarlayacak, biyolojik evrimle sınırlanan insanlar rekabete giremeyecekler. Süper akıllı bir yapay zekâ, hedeflerini gerçekleştirmede son derece iyi olacak ve eğer bu hedefler bizimkilerle uyumlu değilse herhangi bir duygusal neden aramayacak". 'Stephan Hawking'den korkutan açıklama: İnsanlık ortadan kalkacak' (Stephan, 2017) başlıklı haberde "Ünlü bilim adamı Stephen Hawking, "Teknoloji bir noktada insanlardan daha üstün bir noktaya gelecek ve insanları ortadan kaldıracak" ifadelerini kullandı. Saygın bilim-teknoloji dergisi Wired'a konuşan Hawking, "Robot ve bilgisayarların çok gelişmesi bir noktadan sonra insanlığı tehdit eden bir noktaya gelecek. Eğer insanlar bilgisayar virüsü tasarlarsa yapay zekâ bunu geliştirerek, ortadan kaldırabilir" dedi." açıklaması yıllar sonra ünlü bilim adamının fikrini değiştirmediğini gösteriyor. Hatta bu konuda iyimser bir yaklaşım bile sergilemediği düşünülebilir.

Endüstri 4.0, yapay zekâ uygulamaları hayata dair birçok şeyde olduğu/olacağı gibi artık istihbarat olgusunu ve istihbaratın ilgi alanlarını da köklü değişikliklere

uğratmak zorundadır. Uğratmıştır da. Geçmişte bir ülke veya bir yönetici için güç kazanma, savaşta galip olma, egemenlik kurma hususunda önemli olmayan unsurlar zaman içerisinde son derece önemli etkenler haline dönüşmüştür. Örneğin dünyada Ortaçağ olarak isimlendirilen dönemde bir ülke yöneticisi için ilgi beslediği, ele geçirmek istediği ülkenin ne kadar maden yataklarına sahip olduğu, bunların ne kadarını işlettiği çok önemli görülmeyebilirdi. Ama sanayi devrinde o ülkenin işlettiği, işlediği madenin cinsi, miktarı ve sanayi ürünleri üzerindeki etkinliği hayati bir önem derecesine taşınmıştı. Ancak sanayi çağının uzun bir döneminde birey birey insanların alışkanlıkları, kişilikleri çok önemli istihbari değer taşımazken günümüzde artık kişiselden kurumsala kadar her alandaki bilgi değil, bilgi parçacıkları, güç kazanma, küresel egemen olma yolunda son derece önemli unsurlar haline geldi. Dünyanın önemli istihbarat teşkilatlarının bu yeni gerçekliklere yönelik faaliyetler içerisinde bulunduğu biliniyor. İstihbaratı gizlilikten, gizemden biraz daha farklı bir açıya yerleştirmenin önemli olduğu vurgulanıyor. Bu çerçevede, Black ve Morris (2011, s. 15)'in istihbaratın her alandan destek alması ve her alana nüfuz etmesini İsrail istihbaratının değişen niteliği üzerinden açıklamaları, istihbarat faaliyetleri açısından her bilgi alanının önemli, herkesin gözü önünde olan bilginin kullanılmasının da çağın gereği olduğunu ortaya koyuyor: "Orta Doğu anlaşmazlığının ortasında bulunan istihbarat faaliyetlerinin sadece isimsiz ajanlara bırakılması büyük tehlikeler yaratır. İsrail'in Gizli Savaşları, istihbarata hak ettiği ciddiyetle yaklaşmakta ve casusları, gizli ajanları, terörizm ve güvenlik konusunu popüler kurgu dünyası, kasıtlı sızıntılar ve aşırı resmi gizlilikten çıkararak ait oldukları yere, yani tarih, siyaset ve uluslararası ilişkiler bağlamına ve gerçek çağdaş dünyaya yerleştirmektedir."

Ercan Çitlioğlu da (2007, s. 234) istihbarat faaliyetlerinde gelinen noktaya dikkat çekerek, "Geçmişte birbirlerinin askeri güç, kapasite ve savaş yetenekleriyle ilgilenen bloklar yerine günümüzde birbirlerinin ekonomisi, siyasi ve idari yapısı, teknolojisi, sanayii, sosyal yapısı ve dokusu, finans sistemi, doğal kaynakları, inanç ve değer sistemleriyle ilgilenen ve bunları öğrenmek isteyen devletler ve devletler dışı güç odakları ortaya çıktı. Bu radikal değişim ise iletişim ve bilişim teknolojilerinin gelişmesiyle birlikte espiyonaj faaliyetlerinin çerçevesini inanılmaz ölçüde genişleterek çeşitlendirdi." tespitinde bulunuyor.

Hayatın, olayların ve olguların açısı ve niteliği değişince, günlük alışkanlıklarımıza, yaşam formumuza dâhil olan Endüstri 4.0 ile birlikte insanlar kadar nesneler de istihbarat açısından önemli bilgi materyalleri ve kullanıcıları haline dönüşmektedir. Bu alanda da bilgiyi önemli bir etken bileşen olarak görüyoruz. Teknolojinin her şeyden önce bilgi olduğunu vurgulayan Bassala (2013, s. 52) "teknoloji üzerine yapılacak çalışmaların temel birimi, teknolojiyi uygulayan kişiler topluluğudur" çıkarımını yapar. Teknolojiyi kendi çıkarları için kullanmayı düşünen ve onu yaptığı çalışmaların temel birimi olarak kurgulayan insanoğlunun geldiği noktada, ürettiği, geliştirdiği teknoloji insanlığın hizmetinde olma safhasını çoktan aşmak üzeredir ve insanlığı yönetmek, kullanmak üzere

gelişimini sürdürmektedir. Bu husus için her toplumu yönetilecekler kategorine sokamayız (şimdilik, onların da ne olacağı belirsiz gibi duruyor) ama dünyanın çoğu toplumu yönetilmeye ve kullanılmaya doğru yol almaktadır. Bu teknolojiyi icad eden, üreten ve yöneten olmakla ilgili bir alandır.

Elbette her isteyen toplum da teknolojiyi geliştirip insanları ve nesneleri bilgi kaynağı haline getiremez. Bunu sağlamanın olmazsa olmaz bazı şartları vardır. Teknolojik gelişme sağlayabilmenin, icat etmenin bunu toplumsal veya küresel boyuta eriştirmenin en önemli unsurlarından bir tanesi ekonomik güçtür. Ekonominin güçlü olması teknolojik gelişmeyi, bu konuda öncü ve icat eden olmayı tetiklemektedir. Teknolojik icatların küresel boyutlara eriştirilmesi ise ekonomiyi geliştirip zenginleştirmektedir. Yani bu iki unsur birbirini destekleyerek adeta iyice geliştirecek taşıyıcı unsur olmakta ve birbirini karşılıklı güç kaynağı gibi beslemektedir. Elbette ekonomideki çeşitlilik, zenginlik ve güçlülük, teknoloji alanında öncü olmayı, icat etmeyi ve bunları küresel alana taşımayı her zaman sağlamaz. Ekonominizin zenginliğini, birikimini, gücünü artıracak teknolojik icatlara, bu konuda başı çeken lokomotif olmaya yöneltecek farklı unsurlara da ihtiyaç hissedilir. Bu çerçevede kişilerinizin, toplumunuzun belirleyici bir takım değerler sistemine ihtiyacı vardır. Yani teknolojik gelişmeleri, icatları ortaya çıkartacak, yönlendirecek öncelikle bireysel sonra toplumsal bir değerler manzumesine sahip olunması gerekir. Bireysel davranış modelleri, çalışma hissi, düzeni, hırsı bunu toplumsala çevirme ve mâl etme arzusu birbirinin taşıyıcı unsuru olan ekonomi-teknoloji motorunu harekete geçirecek enerjiyi sağlayan en önemli ana faktördür. Fakat, “Teknolojiyi öncelikle insan ihtiyaçlarına hizmet etmesi için geliştirme özgürlüğü, endüstrileşmenin yayılması ve iletişim, ulaşım, güç üretimi ve imalat alanlarında modern mega-teknik sistemlerin geliştirilmesiyle birlikte yitirildi. Muazzam, karmaşık ve birbiriyle ilişkili bu teknolojik sistemler, insani değerleri baştanbaşa istila ediyor ve insan kontrolünü hiçe sayıyorlar. Bu sistemlerde değişiklik, yalnızca verimlilik veya büyük ölçekli teknik değerlerle çatışmadığı sürece mümkün olabiliyor. Bu yüzden, yaşama, çalışma ve oyun oynama biçimlerimiz, modern endüstriyel toplumu yöneten tek parça teknolojik düzen tarafından yapılanıyor (Bassala, 2013, s. 316).” görüşünü de yabana atmamak gerekiyor. İstihbarat faaliyetlerinin de günümüzde bu çerçevede teknolojik düzen tarafından yapılandığını görmemek mümkün değil. Teknoloji bütün bilgi varlıklarını kuşatıp, sarmalayıp yeniden yapılandırırken, temeli bilgi olan bir faaliyet alanının bundan etkilenmemesi düşünülemez.

İşte bu noktada Türk toplumu olarak bizim teknolojiye yüklediğimiz anlam, değer nedir ve bizi nasıl değiştiriyor? sorusuna verilecek cevabımız dünyadaki yerimizi, konumumuzu belirliyor. Teknoloji elle tutulur, müdahale edilir nesneler, materyaller de olsa bizim onlara kişisel veya toplumsal anlamda yüklediğimiz değerler, kullanım amaçlarımız, onun asli yapısını, etkinliğini ve gücümüzün seviyesini ortaya koyacaktır. Ne yazık ki geçmişe ait bu konudaki referanslarımız bize iyi şeyler söylemiyor. Tüm uğraşılarımıza rağmen teknolojinin icad eden, üreten tarafında olmaktan ziyade kullanıcısı olan tarafta olduk. Bu da bizim

bağımsızlığımızı engelleyen bir hareket tarzı olarak yer aldı tarihimizde. Kamran İnan (1999, s. 29)'ın "Türkiye, birçok şey gibi, savunmasını da uzun seneler ihmal etmiştir; dışarıdan yardım olarak ne verilmişse almış, teknolojik üstünlük faktörünü ihmal etmiştir" tespitini diplomatlığı yanında, uzun yıllar yürüttüğü siyasi hayatına ve devlet adamlığına da bağlamamız ve bunu aynı zamanda tespitten öte ciddi bir uyarı olarak da görmemiz gerekir.

Stefan Collini, C. P. Snow'un "İki Kültür (2001, s. 83)" adlı kitabına yazdığı 'Giriş' bölümünde bu konuya biraz daha açıklık getirecek şu görüşleri dile getirir: "Aklı başında hiç kimse temel bir matematik ve fen bilgisine sahip olmanın değerini ve hatta bazı amaçlar için zorunluluğunu inkâr edemez; ama fikirler belli tarihsel ortamlarda iş görürler ve yirminci yüzyılın sonunda büyük sanayi ülkelerinde en önemli ihtiyacın daha fazla bilimsel ve matematiksel ehliyete sahip olmak olduğunda ısrar etmenin, faydası olduğu kadar zararı, hatta tehlikesi olabilir. İstemeden de olsa karar-verme süreçlerini sayılabilen ya da ölçülebilen meselelere indirgemeyi teşvik etmek, yetersiz bir teknolojik ya da istatiksel kavrayış düzeyinde olmaktan rahatsız görünmemekten çok daha zararlı olabilir. Nicelleştirilemeyen kaygılara gerekli ağırlığın verilebildiği bir kamusal dil geliştirme ve yayma ihtiyacı da, en az temel bir bilim bilgisine sahip olma ihtiyacı kadar acildir."

Collini'nin karar verme süreçlerinin sayılabilen veya ölçülebilen düzeyine günümüze yönelik olarak 'kodlanılan'ı da eklemek zaruri olmuştur. Kodlamanın getireceklerini, götüreceklerini, Wells'in (2004, s. 78) ifade ettiği gibi, henüz takip edebilecek, derinliğine çözümleyecek bir araca sahip değiliz. Başkalarının söyledikleriyle seviniyor veya endişeleniyoruz. Ama her halükarda olacaklara hazırlık yapmamız da gerekiyor. Dünyanın geldiği bu noktada yeni küresel emperyalizmin dişlileri arasında sıkışmamak, yapay zekâlara mat olmamak, bireylerin ve toplumun nicelleştirilemeyecek karar verme süreçleri noktasında kaygılarını gidermek, korumak, kollamak için kamusal bir dil ve tavır geliştirme ve yayma görevi devletin tüm kurum ve kuruluşlarının tümünden daha fazla istihbarat teşkilatlarına düşer. Mahir Kaynak, 'Yeni Stratejiler Örtülü Operasyonlar' (2009, s. 14) isimli kitabında zafer kazanmayı yarış atı benzetmesi üzerinden örneklendirerek şu sözlerle açıklar: "İçerde bir zafer kazanmak yarış atı olmaya benzer. Yarışı birisi kazanır ama asıl kazanan yarışla ilgili olan insanlardır. Artık üzerimizden başkalarının kazanmasına izin vermeyelim ve yarış atı olmak yerine at sahibi, jokey, iddiacı gibi rollerden birini oynayalım."

Kaynak'ın analojisinden/benzetmesinden hareketle yarışıp boşuna ter dökmek yerine kazanan olmak için, yapılacak diğer birçok şeyle birlikte, hangi ortamda üretildiğine bakılmaksızın bilgi, bilgi varlıkları, onları elde etmek, tutmak, korumak, bütünleştirmek, kullanmak, derinlemesine değerlendirmek ve bu konuda kamusal bir dil ve tavır geliştirmek de önem verdiğimiz, ciddiye aldığımız uğraş alanlarından olmalıdır. ABD Başkanı Ronald Reagan 'a atfedilen bir söz vardır; "İngilizcedeki en korkutucu dokuz kelime şunlardır, 'Ben hükümet mensubuyum ve buraya size yardım etmeye geldim.'" Bu korkutucu kelimeleri

günümüze uyarlarsak şunları söyleyebilir miyiz?: 'Elektronik dünyasının tüm nimetlerini edindim, ağların tümüne kesintisiz bağlıyım, insanlık en büyük kolaylıkları ve özgürlüğü yaşıyor.' Toplum olarak ülke olarak bu korkuları yaşamak istemiyorsak, bilgiden güç, menfaat elde etmek istiyorsak olması gereken ilk şey, bizi oyun kurucu yapabilecek bilgimizi yönetmektir. Yani, bilginin ve bununla doğru orantılı olarak belgenin yönetilmesi istihbarat eylemini güçlendirir. Etkili istihbarat teşkilatı, sistemli süreçlere sahip ulusal düzeyde işletilebilen belge/bilgi yönetimiyle toplumun ve ülkenin savunmasında daha da güçlü hale gelir.

Bugün "(…) insanlık artık kendini doğadan değil kendi icat ettiklerinden korumak zorunda kalıyor. (…) Teknoloji, yapay da olsa yeni bir doğadır ve bize düşen, eşyanın doğasını dikkate alarak bir yol bulmaktır; yok sayarak hiçbir sorun çözümlenmez; yüzleşerek bir çıkış yolu bulunmalı… Belki de başka bir şeye evriliyoruz, kim bilir? (Fazlıoğlu, 2015, ss. 53-54)." Fakat günümüzde kamu kurum ve kuruluşlarının yönetim sistemlerine ilgisine, yeni teknolojik gelişmelere verdikleri tepkilere baktığımızda görünen o ki yeni dünya gerçekliklerinde, Endüstri 4.0'da, yapay zekâda bizler yine kullanıcı olacağız ve savunmada kalacağız. Sanayileşme döneminde olduğu gibi (Skor: sanayileşmiş ülkeler: 3, Türkiye: 0) bu sefer de endüstriyel mücadelenin kazanan hanesine onlar için '4' yazılırken bize '0' yazılacakmış, geleceğimiz yine başkaları tarafından tasarlanacak, tarihimiz başkaları tarafından şekillendirilecek gibi görünmektedir. Sonucun böyle olmaması için her kuruma, hatta her kişiye, özelde ise istihbarat teşkilatlarımıza çok iş düşmektedir. Geleceğimizi kendimiz tasarlayabilir, kişileri ve toplumları bu yönlendirebilir, teknolojide sadece kullanıcı değil, icad eden ve yönetebilen olursak başarılı olma ve hayatta kalma şansımız yükselecektir. İstihbarat faaliyetlerini bu alanların hiç birisinden uzak tutamayız.

Belge/Bilgi Yönetimi Sisteminin ve Arşivlerin Yapısal Sorunları

Tarihin teknolojiyle birlikte hızlanıp aktığı günümüzde, belgenin/bilginin hayatta kalma, var olma noktasında bir önem arz ettiğini söylemek yanlış olmaz. Bu sebeple hangi kuruma, kuruluşa ait olursa olsun, bilgi varlığı olarak arşiv malzemeleri ve arşivler istihbarat teşkilatlarınca ihmal edilmemelidir. Dünyanın bütün önemli aktörlerinin, güç odaklarının bol bol bilgi bulduğu, malzeme devşirdiği ve ahkâm kesip eylem gerçekleştirdiği bu coğrafyada ülkemizin teşkilatlarının arşivlere, belge/bilgi varlıklarına burun kıvırması, önemsememesi, yapılacak, uğraşılacak bir iş olarak bile sınıflamaması son derece tuhaf değil midir? Belki bu tuhaflık bizim birçok sıkıntımızın sebebi de olabilir. Türkiye'nin özelde istihbarat teşkilatlarının arşivlerle, belgeye/bilgiye bütünlüklü olarak erişimiyle ilgili sorunları var mıdır? sorusunu başka sorularla destekleyerek izah edebilir miyiz?

Herhangi bir kriz durumunda Türkiye için çok hayati olabilecek tüm belge/bilgi birikimlerinin neler olduğu, nerelerde olduğu belirlenmiş midir?

Bunların tümüne kolay ve hızlı erişim sağlanacağından veya onlara uygulanacak muamelelerin eksiksiz yerine getirileceğinden emin olunabilir mi?

Zaman zaman basında ve değişik mahfillerde dile getirilen terör meselelerinin halledilememiş olması, başka ülkelerin operasyonlarına açık olup kolay ajitasyona uğranılması gibi eleştirilerde gerçeklik payı var mıdır? Bu gerçekliğin bütünü içerisinde bir parça olarak görünse de, belgeye/bilgiye erişim ve bunların değerlendirilmesiyle ilgili zafiyetten söz edilebilir mi?

İstihbarat teşkilatları dışındaki kamu kurum kuruluşlarının belge/bilgi güvenliği konularında gösterdikleri umursamazlık, önemsememe, küçümseme gibi davranış kalıpları istihbaratın nitelikli belgeye/bilgiye erişimini ve nitelikli değerlendirilmesini engelleyerek ortak eylemlerde bulunma zafiyeti doğurmakta mıdır? Örneğin ceza evlerinde terör suçundan yatan mahkûmlarla yapılan görüşmeler, psikolojik değerlendirmeler diğer ilgili kurum ve kuruluşlarla ne kadar paylaşılmakta ve değerlendirmeler sonucu ne gibi ortak eylemlerde bulunulmaktadır? Yani ne ölçüde devlet aklı kullanılmaktadır. Milli eğitimin terörün yoğun olduğu bölgelerde elde ettiği bilgiler ne kadar ortak akla aktarılarak eyleme dönüştürülmektedir? Bunlar yalnızca bir takım şablonlara dökülmüş kuru resmi yazışmalar olarak vazife icabı mı mevzuatın belirlediği makamlara iletilmektedir? Yoksa üzerinde detaylı çalışma ve değerlendirmeler yapılıp çözüm ve çıktı odaklı çalışmalar yürütülmekte midir?

Tüm bu soruları cevaplayarak endişeleri giderecek verimli, etkin süreç yönetimi ve denetim mekanizmaları mevcut mudur?

Bu soruların cevapları pek çoğumuzca bilinmektedir, neticede ülkemizde ortak aklın malzemeleri olan arşivlerle, belge/bilgi üretiminden, erişimine ve paylaşılmasına kadar önemli yapısal sorunların olduğunun ipuçları ortaya çıkmaktadır.

Ülke temelinde belge/bilgi yönetiminin üç boyutlu bir yapısal sorunu olduğundan söz edebiliriz. Bunlar; kamu kurum ve kuruluşları ile stratejik öneme sahip organizasyon veya örgütlere ait a-) *belgenin/bilgi varlıklarının hacmi*, b-) tüm bu *teşkilatların içyapısı, işleyiş sistemleri*, bu faaliyet alanına *psikolojik yaklaşımları, meseleye bakıştaki optik kayma* ve c-) kurumlar arası belge/bilginin üretilmesinden, paylaşımına kadar ilerleyen ve devletin ortak aklını ortaya koyacak *koordinasyon ve yönetim sorunu*.

Bir ülkede devletin tüm birimlerine sirayet edecek ve etkili olabilecek bir belge/bilgi yönetiminin devlet sistemi içerisinde hangi düzeyde ve önemde konumlandırıldığı, o ülkenin bilgi toplumu olmasının ve bilgiden nemalanmasının orantısı konusunda da bir göstergedir. Ülkemizde belge/bilgi yönetiminin ve arşivlemenin konumlandırıldığı alanı mercek altına aldığımızda, ciddi bir yapısal sorunlar yumağına sahip olduğumuzu söyleyebiliriz.

Türkiye'nin geçmişten getirdikleri ve güncel ürettikleri belge/bilgi birikimleri hem hacim olarak hem de etkisel özellikleri sebebiyle oldukça yoğunlukludur.

Ancak, her mevkideki çalışanların ve toplamda kişilerin olayı görmekteki aksaklıkları sebebiyle fiziksel hacim ile içerik hacmi arasında doğru ve işe yarar orantı kurulamamaktadır. Türkiye bir hukuk devleti olarak tüm iş ve işlemlerini belgelendirerek kayıt altına almaktadır. Zaman zaman bu husus bürokratik karmaşa olarak nitelense de ufak tefek düzeltmelerle olumsuzlukları giderilebilir haldedir. Ancak neticede devletin aklı olan belgeler, yasal zemine uygun olarak üretilmektedir. Bunların dünya üzerindeki diğer devletlerle karşılaştırması yapıldığında ciddi hacimlerde belge ürettiğimiz söylenebilir. Tüm bu belgeler, devletin işlemsel, operatif ve taktiksel seviyede faaliyetlerinin kayıt altına alınmasının göstergesidir. Bu noktada sıkıntı, yasalara uygun üretmekten ziyade onları doğru sınıflamak, dosyalamak, saklamak, korumak, tekraren kolay ve hızlı erişilebilir kılmak süreçlerinde doğmaktadır. E-belge ve dijitalleştirme bu sıkıntıyı gideren bir kurtarıcı can simidi gibi algılanıp düşünülse de özde bu değildir. Ülke olarak bu noktada da, acemilikten ve belge/bilgi-arşiv meselesini önemsiz addetmekten kaynaklanan optik kaymaya uğramış bir anlayış ile konuya yazılımsal bir ürün ve ticari bir meta boyutunda bakılmaktadır. Kurumların, teşkilatların iş ve işlemleriyle, süreçleriyle uyumlu olmayan, standartlar yayımlanmış olsa da kurumlararası birbirini tanımayan, konuşamayan, anlaşamayan ürünler alınarak veya üretilerek palyatif yaklaşımlarla sorun çözümlenmeye çalışılmaktadır. Meseleye bu açıdan yaklaşıldığı için kurum, kuruluşlar ve organizasyonlar nicelik ve nitelik olarak büyük hacimdeki belge/bilgi yükünü taşıyamamakta, bilgi varlıkları hızla erişilemez, kullanılamaz hale gelmeye doğru yol almaktadır.

Belge/bilgi yönetiminin idari bir uygulama olduğundan uzak bir algılayış ve bunun getirdiği davranış kalıpları, bu faaliyetin en niteliksiz kişilerce yapılabileceği anlayışını kamuda yaygınlaştırmıştır. Bu da üretilen belgenin/bilginin nicelik ve nitelik olarak yönetilmesini en baştan ortadan kaldırmaktadır. Kurumlarda e-belgenin de devreye girmesi ile birlikte fonksiyon çatışmaları da oluşmaktadır. Bilgi işlem ünitelerinin meseleye bir mühendislik olayı tabanından yaklaşması, belge/bilgi yöneticilerini çalışmalara dâhil etmek istememesi sebebiyle süreçlerle ilgili geri dönüşü zor veya masraflı sıkıntılar doğmaktadır. Yanlış bir noktadan başlayan sürecin maalesef koordinasyonunda ve ulusal düzeyde yönetilmesinde de sıkıntılar meydana gelebilecektir.

Belge/bilgi yönetimi süreçleri esas olarak uzmanlık, güvenilirlik, gerektiğinde gizlilik, sorumluluk, idari tecrübe, entelektüel birikim, yasal süreçler hakkında temel bilgi, koordinasyon sağlama yeteneği, teknolojiyi kullanma, iş yapma ve yönetme becerisi gerektirir. Ancak bu işler, bir kurumda niteliği en alt seviyede personelle yürütülmeye çalışılırsa ortaya yönetimden ziyade karmaşa, kargaşa ve kaos çıkacaktır. Ülkemizin bu hususta günümüze kadar hızla ilerlediği reel durum da üzülerek belirtilmelidir ki budur. Yalnız şunu da hatırlatmak da fayda vardır; kaos her zaman kargaşa değildir, yönetilebilirse öngörülemeyen düzen olarak da tanımlanabilir. Kaotik olaylarda, başlangıç durumuna hassas bağlılık bulunur ve çok ufak olaylar çok büyük değişimleri tetikleyebilir. Bu değişimler başlangıç

durumundan sonra ortaya çıkan neticeden çok daha olumlu gelişmeleri doğurabilir.

Devlet Arşivleri Genel Müdürlüğü bugüne kadar kamu kurum ve kuruluşlarına yönelik çok ciddi arşiv çalışmaları yürütmüştür. Arşiv malzemesi tespit çalışmaları ile kamu kurum ve kuruluşlarında üretilen belgelerin tespiti yapılmış, bir anlamda devletin bilgi birikiminin envanteri çıkartılmış, yaptığı işlerin röntgeni çekilmiştir. Bu bilgilerin sınıflandırılması maksadıyla standart dosya planı çalışmaları yürütülmüştür. EBYS denetimleri yapılmıştır. Tüm bu faaliyetlere rağmen kurumlarda her seviyede çalışanlardaki algı yanlışlığı, arşiv ve belge/bilgi yönetimi meselesinin rotasına oturmasındaki en büyük engeldir.

Ulusal düzeyde ele alınacak bir belge/bilgi yönetim sisteminin/sistemlerinin olması gereken yapısına yönelik de şunları söyleyebiliriz:

Gerçeklilik, Yapılabilirlik, Uygulanabilirlik: Belge/bilgi üretiminde veya sisteme dâhil edilecek belgenin bilginin yönetilebilmesi için sistemlerin süreçler, iş akışları, hiyerarşiler, roller, yetkiler, erişim ve paylaşım kriterlerinin ciddi analize dayalı taramalarla tespit edilmesi gereklidir. Hayata geçirilecek sistem/sistemler gerçekçi, kullanılabilir, uygulanabilir, geliştirilebilir olmalıdır. Sorumlulukları ve işlem adımlarını yerine getirmede kolaylık sağlayacak düzenlemeleri barındırmalıdır.

**Sondaj*: Unutulmamalıdır ki, her kurum, her organizasyon, örgüt nev-i şahsına münhasırdır. Bu sebeple tek elden çıkartılmış bir yönetim sistemi gerçekçi olmaz. Her teşkilat kendi faaliyet alanlarını, iş adımlarını, süreçlerini ve muhtemel risk alanlarını iyi yapılmış analize dayalı çalışmalarla bir sondaja tabi tutmalı, açık kapı bırakmadan sistemleştirmelidir. Tüm teşkilatların bunu yapmasından sonra hepsini bütünleştirecek, birbirini tanıyacak, aralarında konuşabilecek sistemle/sistemlerle yönetilebilmelidir.

**Güvenlik, güvenirlik, saklanabilirlik*: Sistemin ürettiği, sakladığı, hizmete sunduğu belgelerin/bilgilerin ikili veya çok taraflı ilişkiler içerisindeki hareketliliğinde güvenliği ile ilgili önlemler alınmış, güvenilirliği noktasındaki endişeleri giderecek yapısallıklar oluşturulmuş, erişim ve paylaşımla ilgili açık kapılar ve riskler, temeli sağlam süreç analizleri ve denetimlerle kontrol altında tutulabilir olmalıdır.

**Kolay kullanılabilirlik, sadelik, basitlik*: Getirilecek sistemler, başlatılacak süreçler, iş ve işlem adımları zorluklar, anlaşılmazlıklar özel uzmanlık alanı gerektirecek bilgiler barındırmamalı, kolay ve basit iş ve işlem adımlarından oluşmalıdır. Özel uzmanlık gerektirecek alanlar elbette olacaktır. Bunlar önceden belirlenerek sisteme gerekirse önlemleri alınarak dâhil edilmeli, bu işlem adımlarını kimlerin kullanacağı veya erişebileceği ile ilgili ilkeler belirlenmelidir.

İstihbarat Faaliyetleri Açısından Gerçekleştirilmesi Gereken Belge/Bilgi Yönetimi İlkeleri

Belge/bilgi yönetiminin istihbarat faaliyetleri açısından başarılı olması için gerçekleştirilmesi gereken birtakım faktörlere gereksinim duyulur. Bu sistemin başarılı olarak kullanılıp işe yarar olmasının temel koşullarından bir tanesi ülke bazında tüm kamu kurum ve kuruluşlarının ortak bir belge/bilgi yönetimi sistemi/sistemleri içerisine dâhil olması ve tavizsiz bunun gerektirdiği süreçleri uygulamasıdır. Stratejik öneme sahip özel işletmelere ve organizasyonlara da hukuki altyapısı oluşturularak bu sistem içerisinde yer açmak gerekir**.** Arzu edilen en üst verimi elde etmek için ise asgari düzeyde şu işlemlerin gerçekleştirilmesi şarttır:

-Belge/bilgi kaynaklarının ve niteliklerinin belirlenmesi,

-Üretilen belgelerin/bilgilerin standart bir çerçevede dosyalanmasının, serileştirilmesinin sağlanması, genel, özel ve dış kodların belirlenerek uygulanmasının temin edilmesi,

-Dosya planı ve saklama planlarının kurumlarda ulusal standart ve kurallara göre tek elden yürütülmesi, değişiklik ve eklemelerin kontrollü yapılması (Burada merkezi bir sistem ve denetimden bahsedilmekle birlikte bunun statikleşmeye sebep olmasına izin verilmeyerek sürdürülebilir politikalarla geliştirilerek ve en önemlisi yasal zemin gözetilerek yürütülmesi gereklidir.),

-Belgelerin/bilgilerin yönetim sistemi içerisinde bir dizinden bir başka dizine, seriye veya dış ortama aktarılması yöntemlerinin tanımlanması,

-Üretilmiş/elde edilmiş hiçbir belgenin, bilgi materyalinin değiştirilememesi,

-Ekip, grup veya ortak çalışma gruplarının çalışmalarına kolaylık ve hızlılık sağlamak amacıyla özelleştirilmiş fonksiyonlara izin vermesi,

- Ekip, grup veya ortak çalışma gruplarının çalıştıkları alanla ilgili her türlü belge/bilgi kaynağına, yetkilendirmeler ve bilmesi gerekenler ilkesi doğrultusunda erişmelerine imkân vermesi,

-Alan bilgilerinde arama yapabilme imkânları sunması, arama ifadelerinin geniş olması, bağıntılı arama yapılabilmesi, altveri-üstveri unsurlarının kapsayıcı, doğruya yönlendirici olması,

-Çalışılan belge/bilgi ile ilgili olarak kullanıcıların başka belge/bilgilerle bağlantı kuracak, çapraz ilişkilendirecek, bütünleştirecek not eklenmesini temin edecek sistemler, yöntemler barındırması,

-Kullanıcıların veya birimlerin erişim hakları, bilmesi gerekenler ilkesi çerçevesinde belgelere/bilgilere erişmesi, yetkisiz kullanıcıların belgenin/bilgi materyalinin kendisine, içeriğine erişememesi, görüntüleyememesi,

-Kullanıcı, arama-listeleme-raporlama fonksiyonlarının geliştirilmesi ve kayıtlarının kesintisiz tutulması,

-Üretilmiş ve süreçlerini tamamlamış tüm belgelerin, elde edilmiş bütün belgelerin/bilgilerin formatlarına, kaynaklarına bakılmaksızın (ancak kaynaklarının kayıt altına alınarak) belirlenmiş kurallar çerçevesinde arşivlenmesi,

-Elektronik ortamlara yönelik olarak bütün dosya formatlama özelliklerini kapsayan arşivleme sistemlerinin oluşturulması, zaman damgalı olarak tutulması, değişik formatların da gerektiğinde sisteme dâhil edilebilir olması,

-Klasik fiziksel ortamda bulunan belgelere/bilgi materyallerine kimlik, yer bilgileri içeren tanımlamalar yapılması, tanımlama bilgilerine göre dizi listesi/envanter oluşturulması, diğer kurumlar, organizasyonlarda üretilen bütünleyici belge/bilgi bağlarının tanımlanması, çapraz ilişkileri verecek dikkat çekecek, bilgilendirecek göndermelere yer verilmesi, tanımlama verilerine göre değişik sorgulamalar yapılmasına, rapor alınmasına, kullanıcı/erişen/kopya alanlara ait kayıtların tutulması,

-Ayıklama-imha işlemlerinin düzenli ve sistemli olarak kontrol altında yapılması,

-Gizlilik ve güvenlik gerektiren belge/bilgilerin niteliklerinin belirlenmesi, bunlarla ilgili mevzuatın güncelleştirilmesi, esnek bir yapıda her zaman güncellenebilir olmasının temin edilip takip edilmesi,

-Sistemin iş, işlem, kullanım süreçlerini gösterir kanun, tüzük, yönetmelik, yönerge, genelge, talimat, direktif gibi yasal ve idari düzenlemelerin yapılarak sistemler üzerinden paylaşılması, gündem ve yeni gelişmelere göre bunların revizyonlarının vakit kaybetmeden gerçekleştirilmesi,

-Kurumlar arası, birimler arası veya kişiler, makamlar arası paylaşım esaslarının belirlenerek kayıtlarının tutulması,

-Kullanıcıların, ilgililerin, yetkililerin bilgilendirilmesi, uyarılması, dikkatinin çekilmesi amacıyla güvenlik ve gizlilik esaslarını da kapsayan aşamalara sahip sistemsel mesaj veya duyuruların oluşturulabilmesi,

-Gizlilik, güvenlik taramalarının sistemli olarak değişik zaman aralıklarında uygulanabilmesi,

-e-imza, m-imza entegrasyonlarının yapılabilmesi,

-Devletin halkın kullanımına açtığı bilgi sistemleriyle de entegrasyon sağlanabilmesi,

-İş ve işlemler esnasında kullanılan formların yönetilebilir olması,

-Raporlama teknikleri ve modülleri desteğinde birim, rol, unvan, kullanıcı bazında detaylı rapor alınması, sağlanmalıdır.

Ayrıca kurumsal veya ulusal düzeyde bu sistemler,

*Belgeyi/bilgiyi güvenli üretme, saklama, dağıtma, paylaşma ve kullanabilme,

*Bütünleştirilmiş ve detay planlama yapmaya yatkın olma,

*Belgeleri/bilgileri etkin yönetme ve verimi artırma,

*Kolay ve hızlı erişim sağlayarak kullanıcılara üst seviyede hizmet sunma,

*Operasyonel, taktiksel veya yönetimsel raporlama, analiz ve anlık sorgulama yapma,

*Planları, tahminleri, senaryoları değiştirme becerisine sahip olarak yeni olasılık senaryoları üretmeye uygun olma,

*Belge/bilgi artışına, yığılmasına, karmaşasına/kargaşasına, felaket senaryolarına alternatif sistem ve süreçleri barındırma,

*Yönetici veya karar vericiler için ihtiyaç hissedilen, sıklıkla kullanılan belgeleri/bilgileri bütünleştirilmiş görüp okuyarak, daha hızlı değerlendirmeye tabi tutmaları, kolay ve etkin karar vermeleri maksadıyla 'yönetici belge/bilgi kompartımanları' oluşturma özelliğine sahip olmalıdır.

Belge/bilgi sistemi kurgulanırken ve kurulurken, sistemi oluşturanlar, süreçleri belirleyenler;

-Kurumların faaliyetleriyle ilgili bütün belge, bilgi, dokümana erişebilmeli, donanım, teknolojik materyaller hakkında gerekli bilgilendirmeleri sağlayabilmeli, tüm personelden iş, işlem ve işleyişle ilgili bilgiler alabilmelidir,

-Üst yönetim de dâhil olmak üzere tüm yönetici kadro ile sıkıntısızca, hızlı ve kolay iletişim kurabilmeli, sübjektif yaklaşımlarla engelleyici ve geciktirici yönetsel müdahaleler olmamalıdır,

-Kişisel veya menfaatlenmelerle ilgili talepleri dikkate almamalıdır.

Ulusal düzeyde belge/bilgi yönetiminin ilk ayağı, kurumsal olarak bu sistemin veya birbirini tanıyan, konuşan, anlaşan sistemlerin hayata geçirilmesidir. Bu sistemin/sistemlerin ulusal düzeyde hayata geçirilmesi için de ilk elden yapılması gereken şey profesyonel belge/bilgi yöneticileri yetiştirmek, kurumlarda istihdam etmektir. Yani bu iki husus birbirini etkileyerek bir döngü oluşturmaktadır. Kurumlarda görevlendirilecek profesyonel belge/bilgi yöneticilerinin özellikleri de genel hatlarıyla şöyle sıralanabilir:

*Belgeyle/bilgiyle ilgili kurumsal yapı ve stratejileri inşa ederek kurumsal performansı, başarıyı artıran, hedeflere erişime katkı sağlayan,

*Belge/bilgi ve iletişim teknik altyapısını kurarak kurumsal belge/bilgi yönetimi mimarisini yapılandıran, bunu ulusal belge/bilgi yönetim sistemine/sistemlerine eklemlendirebilen,

*Kurumsal belge/bilgi politikalarının oluşturulmasına öncülük eden,

*Belge/bilgi ile ilgili kurumsal kararlarda etkili olan,

*Kurumdaki mevcut bilgi varlıkları sayesinde kurumun verimliliğine, başarısına katkıda bulunan, bu katkıyı gerektiğinde ulusal düzeye taşıyabilen,

*Kurum içinde veya mevzuatla ve belirlenmiş diğer kurallar çerçevesinde paydaşlarla, yatay-dikey iletişim ve paylaşım kanallarının sürekli açık tutulmasını sağlayan,

*Yöneticiler ile kurum çalışanları, katılımcıları, paydaşları arasındaki her türlü (sözlü/sözsüz) belge/bilgi akışının sürdürülebilirliğini ve güvenilirliğini denetleyen,

*Kaos ve belirsizlik oluştuğunda olumsuzlamadan, paniklemeden bunu bir fırsat olarak gören,

*Çok sayıda birbiri ile etkileşen yeni manevra alanları oluşturarak çabuk yanıt veren esnek yapılar inşa edebilen,

*Bireyleri, çalışanları yalnızca pasif elemanlar olarak değil, organizasyonun kendisi olarak gören,

*Kurumunun iş yapış tarzını, hassasiyetlerini, etkileşim ve etkileme gücünü bilen ve geniş bakış açısı kullanarak kurumun özgün dokusunu oluşturmayı başaran,

*Gerektiğinde işbirliği içinde sistemi değiştirerek yeni paradigmalar oluşturan,

*Yeni değerler geliştirip risk üstlenenler,

*Bütüncül bakış açısı, sinerjik düşünme ve hızlı karar verme yeteneklerini geliştirmiş olan,

*Bilgi sağanağından anlamlı ve önemli olanları ayırt ederek belgeleri/bilgileri bütünleştirebilen,

*Dış partnerleri ve değişim dinamiklerini yakından takip eden,

*Çoklu etkileşimin bulunduğu kompleks süreç ve olguları algılama ve sağlıklı karar verebilme yetisini geliştirmiş olan,

*Dışsal veri ve enformasyonu bilgiye dönüştürerek kurumun bundan azami fayda sağlamasına imkân verecek düzenlemeleri yapan kişiler, "belge/bilgi yöneticisi" olarak adlandırılabilirler.

Kazanımlar

Bu çerçevede belge/bilgi yönetim sistemlerini kurgulayıp, sistematik olarak çalıştırdığımızda birçok açıdan fayda sağlamakla beraber özelde istihbarat disiplini açısından özetle ilk elden şu faydaları sağlarız:

Bu konuda ilk elden söylenecek şey sistemli belge/bilgi yönetimi "istihbarata karşı koymanın" en önemli araçlarından bir tanesidir. Gerektiği gibi kurgulanıp

ulusal düzeyde kullanıldığında istihbarata karşı koyma eylemlerinin sağlıklı yürütülmesini temin eder. İstihbarata karşı koyma, bir devletin istihbarat kurumunun, düşman ya da düşmanca tavırları olan yabancı istihbarat kurumlarının veya zararlı örgüt ve organizasyonların söz konusu devlete karşı istihbarat yapmalarına engel olması olarak tanımlanır. Burada iki önemli ayrıntıdan söz edebiliriz. Birincisi, düşman devletlerin istihbarat birimleri tarafından yapılan istihbarat çalışmalarının devletin 'sırları' olarak bilinen belgelere/bilgilere erişimini/ulaşımını engellemek; diğeri ise, devletin 'sırlarını' bilen insanların korunmasını sağlayarak bu insanların yabancı istihbaratlara – bilinçli veya bilinçsiz- erişmelerine/ulaşmalarına, belge/bilgi aktarmalarına engel olmak. Sistemli bir belge/bilgi yönetim süreci bu iki ayrıntı konusunda istihbarat birimlerine çok ciddi katkılarda bulunur. Amerikan istihbaratıyla ilgili incelemesinde Ersanel (2006, s. 39) şu tespitte bulunur: “Dünyanın en büyük gücü bilgiyle çözülebilir. Çünkü bilgiyle kuruldu.” Bir istihbarat teşkilatı da bilgiyi elde edip üst seviyede değerlendirip kullanırsa çözemeyeceği bir mesele olmayacaktır.

Elektronik tabanlı, ağlar üzerinde gelişen gerçeklikler bildiğimiz uzmanlık paradigmasını güçsüzleştirmektedir. İstihbarat teşkilatlarının bu çerçevede bu ortamlarda oluşan bilgi trafiğine uyum sağlayacak, hızlı değerlendirmelere zemin hazırlayacak, çok hızlı ve çok yaygın etkiler oluşturacak değerlendirmeler yapabilecek yeni nesil uzmanlara ve bu uzmanları belge/bilgi ile destekleyecek, süreçleri bütünleştirecek, paylaştıracak sistemlere ihtiyacı olacaktır. Belge/bilgi yönetim sistemleri yeni nesil uzmanların gelişimine katkı verecek, belgeyi/bilgiyi organize ederek, örgütleyerek, bütünleştirerek, paylaştırarak, kolay ve hızlı erişim sağlayarak, uyararak destekleyecektir.

Sonuç

Belge/bilgi yönetim sistemi, her kademedeki çalışan ve yöneticilerin iş üretme, yürütme, bilgiye erişim ve kullanım biçim, yöntem ve işleyişine tüm adımlarda eşlik edip bunları doğrudan etkileyip gerektiğinde müdahale ettiği için yönetim etkinliğinin bir parçasıdır. Ulusal veya kurumsal faaliyetlerin etkinliğini, bilgi kaynaklarının kullanımını izleme, denetleme faaliyetlerini takip etmek konusunda aktif bir rol oynar. “Bilinmezliklerin giderilmesi, doğal olarak daha iyi kararlara yol açar, bu kararlar yapılacak doğru seçimlerle bir sektörün, bir kurumun veya bir ülkenin kaderini tayin eder (Özdemirci, 1996, s.30).” Bu çerçevede belge/bilgi yönetim sistemlerinin ulusal düzeyde süreçlerinin tanımlanarak işler hale getirilmesi, istihbarat kurumlarının da etkin olarak destekledikleri ve öncelikli olarak hayata geçirilmesini hedefledikleri konulardan olmalıdır. Bu destek makine ile insanın savaşının başladığı bugünlerde daha önemli hale gelmiştir. “bilim bir ürünün fiziksel olasılık sınırlarını belirler; ama asla bu ürünün nihai şeklini tanımlamaz veya bu konuda bir direktifte bulunmaz” görüşündeydi Bassala (2013, s. 146). Ama geldiğimiz şu noktada bilim artık ürünün nihai şeklini

belirlediği gibi, ürünün de insanla ilgili unsurları, hayat formlarını belirleyeceği dönemlere doğru evrilmektedir. Bilimin nihai şeklini belirlediği teknolojinin, insanlığa hizmet ederek onu daha da rahata erdirecek, güvenliğini, esenliğini artıracak bir yapıda gelişmesi yerine, 'yapay zekâ' gibi –ne gariptir ki yine insan eliyle- insanlığın gözetleneceği, denetleneceği, yönetileceği, belki ezileceği bir kulvarda ilerlemektedir. Buna yönelik öngörüler literatürde yoğunluklu olarak yer almaya başlamıştır. Dikkat çekici olanlardan bir tanesi yine Bassala'nın tespitleridir: (2013, s. 316) "Teknolojiyi öncelikle insan ihtiyaçlarına hizmet etmek için geliştirme özgürlüğü, endüstrileşmenin yayılması ve iletişim, ulaşım, güç üretimi ve imalat alanlarında modern mega-teknik sistemlerin geliştirilmesiyle birlikte yitirildi. Muazzam, karmaşık ve birbiriyle ilişkili bu teknolojik sistemler, insani değerleri baştanbaşa istila ediyor ve insan kontrolünü hiçe sayıyorlar. Bu sistemlerde değişiklik, yalnızca verimlilik veya büyük ölçekli teknik değerlerle çatışmadığı sürece mümkün olabiliyor. Bu yüzden, yaşama, çalışma ve oyun oynama biçimlerimiz, modern endüstriyel toplumu yöneten tek parça teknolojik düzen tarafından yapılanıyor."

Bilginin bilgiyle savaşı olan istihbarat mücadeleleri bundan sonraki süreçte makine bilgisi ile insan bilgisi arasında geçecek gibi görünmektedir. "3. Dünya Savaşı'nda hangi silahların kullanılacağını bilmiyorum ama 4. Dünya Savaşı'nda taş ve sopalar olacağını biliyorum" diyordu Albert Einstein. İnsan-makine çatışması bizleri taş ve sopaya döndürecek midir? bunun da yakın zamanda emareleri görülecektir diye düşünüyorum. Yapay zekânın insanlığa karşı tehlikeler getireceğinden endişelenenlerin de buna karşı 'insani kolektif zekâyı' ortaya koyması gerekiyor.

Türkiye olarak bizim geliştireceğimiz insani kolektif zekânın ana kod kaynaklarından bir tanesi kuşkusuz belge/bilgi birikimlerimiz olacaktır. Bunların aktif ve nitelikli kullanımı bilginin bilgiyle savaşının ana unsuru olarak istihbarat teşkilatlarının elini rahatlatacak önemli bir silahtır. Toplumsal 'kolektif insani zekâmız'ın temeli olacak belgeyi/bilgiyi yöneterek geliştireceğimiz yeni kodlarla 'yapay zekâyı' insanımızın, toplumumuzun, devletimizin her açıdan güçlenmesine katkı sağlar hale getirebiliriz. Ve yapay zekâ bilgisi ile insani zekâ bilgisinin mücadelesinde kazanan biz olabiliriz. Ancak bunun için elimizdeki en eski belge/bilgi kaynakları ve materyallerinden başlayarak onları kayıt altına alıp öncelikle niteliklerini belirlememiz, korumamız, yönetmemiz, gereken koşullarda paylaşmamız gerekiyor. Toplumumuzun, insanımızın, devletimizin, kültürümüzün velhasıl her şeyimizin selameti ve güvencesi için bu ihmal edilebilir ve geciktirilebilir bir eylem olmaktan çıkmış ölüm-kalım mücadelesine dönüşmüştür.

Kaynakça

AKSU, Halil ve CANDAN, Uğur ve ÇANKAYA, Mehmet Nuri (2011). Her Şey Çıplak. İstanbul: MediaCat Kitapları.

BASSALA, George (2013). Teknolojinin Evrimi. Ankara: DOĞUBATI Yayınları.

BLACK, Ian ve MORRIS, Benny (2011). İsrail'in Gizli Savaşları. İstanbul: Pegasus Yayıncılık.

BAUMAN, Zygmunt (2015). Akışkan Modern Dünyada Kültür. Ankara: [a]tıf Yayınları.

ÇAKIROĞLU, Mustafa (2017). "Network Teorisi ve Sosyal Ağların Çıkış Hikayesi", http://asdfghjklavye.com/tag/6-derecelik-ayrim/, Erişim: 12 Kasım 2017).

ÇEVİK, Abdulkadir (2002, Kış). Küreselleşme ve Kimlik. Avrasya Dosyası Jeopolitik Özel, cilt: 8, sayı: 4. Ankara: ASAM Yayınları.

ÇİTLİOĞLU, Ercan (2007). Gölgedeki Sessiz Tanıklar. İstanbul: Doğan Kitap.

DOLGUN, Uğur (2015). Şeffaf Hapishane Yahut Gözetim Toplumu. İstanbul: Ötüken Yayınları.

DUDLEY, Leonard M. (1997). Kalem ve Kılıç. Ankara: Dost Kitabevi Yayınları.

ERDAL, Ekin (2017). Tesla Kasırgadan Önce Florida'daki Araçlarının Bataryalarını Arttırdı! http://www.webtekno.com/tesla-kasirgadan-once-florida-daki-araclarinin-yol-suresini-arttirdi-h33460.html (Erişim: 17 Ekim 2017).

ERSANEL, Nedret (2006). Amerikan Ruhunun Menfaat Fihristi PaRDes.. İstanbul: Hayy kitap.

FAZLIOĞLU, İhsan (2015), Soruların Peşinde. İstanbul: Papersense Yayınları.

FEENBERG, Andrew 2010). Eleştirel Teknoloji Teorisi Genel Bir Bakış. {Editörler: Guidio Ruivenkamp ve Joost Jongerden ve Murat Öztürk. Teknoloji ve Toplum içerisinde}. İstanbul: Kalkedon Yayınları.

GATES (2015): İnsanlık yapay zekadan kaygı duymalı (30 Ocak 2015). http://www.bbc.com/turkce/haberler/2015/01/150130_gates_yapay_zeka. Erişim: 2 Eylül 2017).

GOTTMANN, Jean (2003). Bugeaud, Gallieni, Lyautey: Fransız Sömürge Savaşlarının Gelişmesi. [Editör: Edward Mead Earle]. Ankara: ASAM Yayınları.

HALEVY, Efraim (2008). Karanlıktaki Adam. İstanbul: Profil Yayıncılık.

HARDT, Michel ve NEGRİ, Antonio (2008). İmparatorluk. İstanbul: Ayrıntı Yayınları.

HİÇYILMAZ, Ergun (2008). Operasyon MİT CIA MOSSAD KGB. İstanbul: Bilge Karınca Yayınları.

İNAN, Kâmran (1999). Hayır Diyebilen Türkiye. İstanbul: TİMAŞ Yayınları.

KAHN, David (2002, Yaz). İstihbaratın Tarihsel Teorisi. Avrasya Dosyası İstihbarat Özel, cilt: 8, sayı: 2. Ankara: Avrasya Bir Vakfı Yayınları.

KAYNAK, Mahir (2009). Yeni Stratejiler Örtülü Operasyonlar. İstanbul: Truva Yayınları.

KELLY, Mark G. E. (2016). Uluslararası Biyopolitika Foucault, Küreselleşme ve Emperyalizm. Ankara: pharmakon yayınevi.

KOÇER, Kemal (2003). Ulusal Kurtuluş Savaşında M. M. Örgütü'nün Gizli Eylemleri. İstanbul: Özne Yayıncılık.

LEE, Elizabeth (2017, Temmuz). Zihinlerarası Savaş Dönemi Geliyor Teknoloji, Beyinlerarası İletişimi Sağlayabilecek mi? Turquie Diplomatique, sayı: 99, İstanbul.

MUSK, Elon (2017, Eylül). Yapay Zekâ, 3. Dünya Savaşını Çıkartabilir. Turquie Diplomatique, sayı: 101, İstanbul.

ÖZDEMİRCİ, Fahrettin (1996). Kurum ve Kuruluşlarda Belge Üretiminin Denetlenmesi ve Belge Yönetimi. İstanbul: Türk Kütüphaneciler Derneği Yayını.

PENROSE, Roger (2015). Kralın Yeni Aklı. İstanbul: Koç Üniversitesi Yayınları.

ROOF, Heather M. (2017, Temmuz). Teknoloji, Değerler ve İnsan Güvenliği Yapay Zekâ Yoluyla İnsan Güvenliğinin İlerletilmesi. Turquie Diplomatique, sayı: 99, İstanbul.

SNOW, C. P. (2001). İki Kültür. Ankara: TÜBİTAK Popüler Bilim Kitapları.

STEPHAN (2017) Hawking'den korkutan açıklama: İnsanlık ortadan kalkacak.http://www.mynet.com/haber/dunya/stephan-hawkingden-korkutan-aciklama-insanlik-ortadan-kalkacak-3365136-1. Erişim: 3 Kasım 2017)

TANIŞ, Tolga. Türkiye siber savaşa hazır mı? Richard A. Clarke ile söyleşi. Hürriyet Pazar. 29 Nisan 2012.

TORUNLAR, Mehmet (2016). İletişim/Bilgi Çağında Endişeli Bir Hayalperestin Gözünden Bilimsel ve Teknolojik Gelişmeler. Yeni Türkiye, 88, ss. 417-434.

UÇKAN, Özgür ve ERTEM Cemil (2011). WIKILEAKS Yeni Dünya Düzenine Hoşgeldiniz. İstanbul: Nesil Yayınları.

WALLERSTEIN, Immanuel (2013). Bilginin Belirsizlikleri. İstanbul: Sümer Yayıncılık.

WELLS, H. G. (2004). Dünya Devrimi Üzerine Açık Komplo. İstanbul: Anka Yayınları.

EBYS Uygulaması e-Arşiv midir? TÜRKSAT–Ankara Üniversitesi BEYAS Koordinatörlüğü e-Arşiv Deneyimi ile Yeni Yaklaşımlar

Prof. Dr. Fahrettin ÖZDEMİRCİ
Ankara Üniversitesi Belge Yönetimi ve Arşiv Sistemi (BEYAS) Koordinatörü

Ahmet SAVAŞ
TÜRKSAT A.Ş. Yazılım Geliştirme Direktörü

Uzm. Zeynep AKDOĞAN
Ankara Üniversitesi BEYAS Koordinatörlüğü; Ankara Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı Doktora Öğrencisi

Öz

EBYS uygulamaları e-Arşivin oluşumunu sağlayan süreç uygulamasıdır. EBYS Uygulamasın öncelikli işlevi, kurumların yasal yükümlülüklerini, üstlendiği işlevleri yerine getirirken gerekli olan belgelerin e-ortamda üretim sürecini gerçekleştirmektir. Yani belge öncelikle yasal ve idari amaçlar için üretilerek yönetim eyleminin gerçekleştirilmesi sağlanmaktadır. Kurumun belleğini oluşturan arşivler, yalnızca EBYS Uygulamasında üretilen belgeleri içermezler. Kurumsal belleği oluşturan arşiv materyal ve malzemeleri farklı özelliklere, farlı üretim ve oluşum süreçlerine, farklı içeriklere, farklı işlevlere sahiptir. Kurumsal işlev ve süreçlerin kimi zaman bir parçası, kimi zaman sürecin kendisi, kimi zaman sürecin tamamlayıcısı olan, fotoğraflar, ses kayıtları, video kayıtları, objeler, kurumun verdiği diploma, berat, kanıtsal belgeler, tapular vb. kurumsal belleğin ayrılmaz parçalarını ve estetiğini oluşturmaktadır. Bu bağlamda geniş bir yelpazeye sahip kurumsal belleğin, öncelikle yönetimsel işlevlerin gerçekleştirildiği bir EBYS platformunda yönetmek zor, hatta imkânsız görünmektedir. e-Arşiv kurumsal belleği oluşturan varlıkların yönetimini gerektirmektedir. Kurum ve kuruluşlar EBYS kullanmaya yönlendirilmektedir. Kurumlar buna hazır mı? e-Arşivin boyutu doğru algılıyor mu? e-Arşiv nedir? Yapısı, kapsamı, fonksiyonları, aksiyonları ne olmalıdır? Çalışma, EBYS ve e-Arşivin ilişkisi, boyutu, etki alanı ile yeni yaklaşımlar ve çözümlere yönelik genel bir bakış açısı sağlamayı hedeflemektedir. Bu kapsamda TÜRKSAT tarafından geliştirilen Arşivnet yazılımı ile Ankara Üniversitesi'nde başlatılan pilot uygulama deneyimi paylaşılacak, e-arşiv uygulamasının bileşenlerine ve boyutlarına dikkat çekilmektedir. Belgenin e-ortamda etkin, güvenilir üretimi ve yönetimi için bize platform sunan EBYS uygulamaları mücadeleyi kazanmak üzere, ancak e-Arşivin mücadelesi ise yeni başlamaktadır.

Anahtar Sözcükler: *Elektronik Belge Yönetimi, Elektronik Arşiv, Ankara Üniversitesi, BEYAS Koordinatörlüğü, Arşivnet, TÜRKSAT*

Giriş

Günümüzde bilginin üretim ve kullanım süreçleri, yenilikçi bilgi teknolojilerini kullanmayı gerektirdiğine göre, belge yönetimi ve arşiv alanında da yenilikçi bilgi teknolojilerini kullanmak zorundayız. Biz şu anda değişimin ve dönüşümün tam içinde yer alıyoruz. Bu bağlamda değişim ve dönüşümün olmadığı dönem yoktur, değişimi ve dönüşümü yönetemeyenler vardır. O halde yenilikçi teknolojilerin beraberinde getirdiği riskleri bertaraf ederek iş ve işlem süreçlerinde EBYS'leri kullanmak ve e-Arşiv sistemlerini kurmak zorundayız. Elbette riskleri bileceğiz, önlemlerimizi alacağız ve çağımızın gerektirdiği yöntem ve teknikleri kullanarak EBYS ve e-Arşiv sistemlerini yöneteceğiz. Bunu başaramazsak işte o zaman risk ve tehditler bizim kâbusumuz olacaktır. Risk ve tehditleri fırsata dönüştürmek için çalışmalıyız.

EBY Sistemleri, kurumlara sağladığı kazanımlarla daha geniş kapsamda kamunun idari işleyişinden, tarihsel, fonksiyonel ve hukuki yükümlülüklerinin yerine getirilmesine kadar geniş bir yelpazede yardımcı olmaktadır. Günümüzde kuruluşlar bu yükümlülükleri yerine getirirken bir değişim ve dönüşüm sürecine girmektedir. Bu anlamda EBYS, e-devlet entegrasyonunda kurumların iş ve işlemlerinin dijital ortamda gerçekleştirmelerine yönelik e-kurum dönüşümlerinin merkezinde durmakta ve temel bileşenler arasında yer almaktadır. Kontrolsüz birikim ile büyüyen belge yığınları zaman içinde yönetilemez hale gelmektedir. Gelen-giden belgenin izlenememesi ve yönetilememesi sonucunda kaybolması, iş süreçlerinde gecikme ve karışıklığın doğması, depolama ve erişim için ek maliyet getiren harcamalara neden olmaktadır. İşlemlerini bütünüyle dijital ortamda gerçekleştirmeyi hedefleyen kuruluşlar için e-kurum yapılandırmasında maliyeti düşürme ve verimliliği artırma önemli bir göstergedir. Kurumsal bilgi sistemlerinin entegre biçimde yapılandırılması teknik olduğu kadar stratejik bir yönetim anlayışı da gerektirmektedir (Özdemirci ve diğerleri, 2013, s.24)

Kamu kurumlarının 31.07.2017 tarihine kadar, Üniversite ve Belediyelerin ise 31.12.2017 tarihine kadar EBYS'ye geçmesi için Başbakanlık Müsteşarlığının Mayıs 2017'de aldığı karar göz önüne bulundurulduğunda, EBYS uygulamalarının tüm kamu kurum ve kuruluşlarını kapsayacağı açıktır. 2017/21 sayılı e-Yazışma Projesi konulu Başbakanlık Genelgesi'nde 158 kamu kurum ve kuruluşunun EBYS kullanmaya başladığı belirtilmektedir (e-Yazışma Projesi, Genelge, 2017)

Kamu kurum ve kuruluşlarının EBYS kullanmaya yönlendirilmeleri, e-Arşivlerin de hızla gündemimize girmesine neden olmaktadır. Ancak kurumlar bunlara (EBYS ve e-Arşiv) hazır mı? Kurum Arşivleri e-Arşive hazır mı? Dahası Milli Arşiv buna hazır mı? e-Arşivin boyutu doğru algılıyor mu? e-Arşiv nedir? Yapısı, kapsamı, fonksiyonları, aksiyonları ne olmalıdır? e-Arşiv için beklemek zorunda mıyız? Ne kadar zamanımız var? Bence hiç zamanımız yok. Bunlar açıklığa kavuşturulması gereken hususlar olarak karşımızda durmaktadır.

Elektronik Belge Yönetim Sistemi (EBYS) ve e-Arşiv Sistemi

EBYS uygulamasının, rutin yazışmaların yapıldığı bir yazılım ve çıktılarının da rutin yazışma evrakı olarak değerlendirilmesi bir kaostur ve ciddi krizlerin habercisidir. EBYS, iyi yönetilemezse, yönetim için ciddi krizler çok yakın demektir. Başarısız yönetimi, iyi tanımlanmamış iş süreçlerini EBYS uygulamaları düzeltemez. EBYS uygulamasının öncelikli işlevi, kurumların yasal yükümlülüklerini, üstlendiği işlevleri yerine getirirken gerekli olan belgelerin e-ortamda üretim sürecini gerçekleştirmektir. Yani belge öncelikle yasal ve idari amaçlar için üretilerek yönetim eyleminin gerçekleştirilmesi sağlanmaktadır. EBYS uygulamaları, e-Arşivin oluşumunu da sağlayan süreç uygulamasıdır. Yönetim süreçlerinde üretilen belgeler işlevlerini yerine getirdikten sonra, (yasal, idari ve yönetimsel) kurumsal belleğin bir parçası olarak arşivde ikinci yaşamına başlar. Bu ikinci yaşamda, belgenin görmesi gereken işlemler, üstlendikleri işlevler, erişim ve kullanım yetkileri gibi fonksiyonlar değişikliğe uğrar. Aynı zamanda kurumun belleğini oluşturan arşivler, yalnızca EBYS Uygulamasında üretilen belgeleri içermezler. Kurumsal belleği oluşturan arşiv materyal ve malzemeleri farklı özelliklere, farlı üretim ve oluşum süreçlerine, farklı içeriklere, farklı işlevlere sahiptir. Kurumsal işlev ve süreçlerin kimi zaman bir parçası, kimi zaman sürecin kendisi, kimi zaman sürecin tamamlayıcısı olan, fotoğraflar, ses kayıtları, video kayıtları, objeler, kurumun verdiği diploma, berat, kanıtsal belgeler, tapular vb. kurumsal belleğin ayrılmaz parçalarını ve estetiğini oluşturmaktadır. Nasıl ki sanat ve estetiğin gelişimi birbirini besleyen süreçler olmuştur, görsel malzeme de kurum tarihinin estetiğidir, kurum belleğinin tamamlayıcısıdır. Bunun göz ardı edilmemesi gerekir. Salt iş ve işlem süreçlerinden kaynaklı oluşan arşiv belgelerinden ibaret bir arşiv estetikten uzak, donuk kurumsal bellekler bırakmaktan öteye geçemez. Bu bağlamda geniş bir yelpazeye sahip kurumsal belleğin, öncelikle yönetimsel işlevlerin gerçekleştirildiği bir EBYS platformunda yönetmek zor, hatta imkânsız görünmektedir. e-Arşiv kurumsal belleği oluşturan bilgi varlıkların yönetimini gerektirmektedir.

Uluslararası gelişmelere paralel olarak Türkiye'de yaşanan hızlı değişim ve dönüşümün etkisiyle geçmişe odaklı arşiv uygulamalarından, güncel bilgi ve belgenin üretiminden yönetilmesine kadar geçen bütün süreçleri kapsayan, uluslararası yönleri olan, **bilgi→güç** odaklı arşivcilik anlayışına doğru bir geçiş yaşanmaya başlanmıştır. (Özdemirci, 2017, 199-200.s.).

EBYS uygulamaları, belgenin e-ortamda etkin, güvenilir üretimi ve yönetimi için bize platform sunmakta, EBYS deneyimlerimiz bizi her geçen gün daha ileriye götürmektedir. Deneyimlerimiz vardığımız yer değil, gittiğimiz yol olarak değerlendirilmelidir. Yolda yaşadıklarımız, bizi değiştirmekte ve geliştirmektedir. EBYS mücadeleyi kazanmak üzere, ancak e-Arşivin mücadelesi ise yeni başlamaktadır. Bu bağlamda TS 13298 Elektronik Belge ve Arşiv Yönetim Sistemi" standardı 2015 revizyonu ile bu açıdan önemli bir yaklaşım getirmektedir (TS 13298, 2015). Standardın arşiv yönetim kısmı her geçen gün

gelişecek ve ihtiyaçlara cevap verecek şekilde geliştirilecektir. Yolculuğa dikkat ettiğimiz sürece gelişebiliriz. e-Arşivi, EBYS ile entegre çalışması gereken bir sistem olarak yapılandırmak zorundayız.

e-Arşiv Sistemlerinde Tanımlama ve Erişim

EBYS' lerde daha çok belge temelli erişim ve kullanım ön planda iken, e-Arşiv sistemlerinde erişim daha çok bilgi temelli olacaktır. Bu da e-Arşiv sistemlerinde tanımlama yöntemlerinin, erişim stratejilerinin ve erişim yetkilerinin buna göre yapılandırılmasını gerektirmektedir. Fon, seri, klasör, dosya bazlı yönetim temelinde koleksiyon bazlı tanımlama ve yönetim (fotoğraf, video, resim, pul vb. koleksiyonları), obje bazlı tanımlama ve yönetim (müze malzeme ve materyalleri vb.), arşiv malzeme türlerine göre tanımlama, erişim, kısaca kurumsal belleği oluşturan bilgi varlıklarının yönetimi e-Arşivin bileşenlerini oluşturmaktadır. Bu noktada EBYS'lerde olduğu gibi e-Arşiv sistemlerinde de tanımlamanın ilk unsurunu belgeyi üreten birim oluşturmalı, konu/fonksiyon bundan sonra gelmelidir. e-Arşiv sistemleri bu yönüyle koleksiyon düzenleme ve tanımlamada diğer bilgi merkezlerinden ayrılmakta ya da ayrışma noktasını oluşturmaktadır. Hangi yapıda koleksiyon oluşturulursa oluşturulsun, unutulmaması gereken temel nokta, belgenin aidiyetinin ilk unsur olduğudur. O halde e-Arşiv sistemlerine ilişkin yazılımlar kurgulanırken, temel mimari ve kurgu buna göre yapılandırılmalıdır.

Belge-bilgi **üretene değil, ihtiyacı olana** aittir. Ancak **üretenin bilinmesini, tanımlanmasını, takdir edilmesini** gerektirir. **Aidiyet** bilginin **niteliğinin belirlenmesindeki** en temel unsurdur. Belge-bilginin **tanımlanmasına, düzenlenmesine ilişkin yapılan** tüm çalışmalar, **iki yönlüdür** ya da **iki amaca** hizmet eder: **(1) Bilgiye ihtiyacı olanı eriştirmek,** (2) **bilginin kaynağını belirlemektir**. Zira erişemediğiniz bilgi sizin değildir. e-Arşiv sistemleri yalnızca belgeye değil, bilgiye erişimi sağlayan; aidiyeti kaybetmeden belgeler arasındaki yatay ,dikey ve çapraz ilişkileri tanımlayabilen ve sorgulayabilen bir yapıda olmalıdır. Arşivlerde **bilgiye erişim**, arşiv belgelerinin **tanımlanmasında olduğu gibi**, kendi içinde **farklı paradigmalara sahiptir**, ya da kendi içinde **yeni paradigmalar** (değerler dizisi) oluşturması gerekir. Bu bağlamda arşivci **bilgiyi tanımlarken ve sunarken**, bilgiye **erişimle ilgili güvenlik** süreçlerini ve yetki düzeylerini de bilmeli, oluşturmalı ve yönetebilmelidir. Arşivler kurumsal veriler temelinde değerlendirilmekle birlikte sıklıkla göz ardı edilen kişisel veri barındırdığı hususudur. Dolayısıyla e- arşivler farklı açılardan analiz edilmesi gereken veri barındıran sistemlerdir.

Belge Merkezleri ve Arşivler, geleceğin 'Veri Merkezleri'dir. Artık 'Kurum Arşivi' olmayacak, 'Kurum Veri Merkezi' olacak, bu veri merkezlerinde biz belgeyi nasıl yönetiriz. Sanırım üzerinde durulması gereken önemli hususlardan birisi de budur. (Özdemirci, 2017, 229.s.).

EBYS- e-Arşiv farlılıklarını kısaca vurgulamak gerekirse;

- Barındırdığı belge türleri/bilgi kaynakları farklıdır.
- Metadataları farklıdır.
- Kullanım amaçları ve karşıladıkları ihtiyaçlar farklıdır.
- Erişim süreçleri ve yetkileri farklıdır.
- Hizmet sunum biçimleri farklıdır.
- Güvenlik süreçleri farklıdır.
- Arama stratejileri ve yöntemleri farklıdır.
- Farklı tanımlama unsurlarını belirlemeyi gerektirir.

e-Arşiv Sistemini Gerektiren Nedenler ve Yenilikçi Bilgi Teknolojileri Kullanımı

Belge yönetimi ve arşivin uygulamalarının nesnesi söylem değil, belge üzerinde varlığını canlı bir şekilde sürdüren bilgidir. Dolayısıyla belge yönetimi ve arşivin uygulamalarının amacı, belgeyi tüketmek/ yok etmek/ hapsetmek değil, bunun yerine bilginin varlığının ne demek olduğunu göstermektir. Belge yönetimi ve arşiv, geçmişin aslında ne kadar da bugüne ait bir şey olduğunu göstermektedir. Artık belge yönetimi ve arşivler bilgi sistemlerinin ve bilişim yönetiminin en önemli ve en büyük alanını oluşturmaya başlamış, bilgi sistemlerin baş aktörü haline gelmiştir.

Arşiv çoğu zaman bizim içinde yaşamadığımız geçmişe götüren bir varlık, bir zaman dilimidir. Teknik ve zaman açısından geçmiş olarak ifade edilse de şimdi olarak vardır. Arşivler, kurumlar, alanlar, siyasal olaylar üzerinde bilgiyle/belgeyle ilişki kurar. Bir yöntem olarak arşiv geçmiş, şimdi ve gelecek arasındaki ilişkinin anlaşılmasına yardımcı olur. Bu bağlamda kurumsal, toplumsal hafızanın bu kısmına geri gitmek ve şimdiye ulaşmanın tek yoludur. Bu anlamda arşiv, tarihi yeniden yazmak için anlatılmamış ya da yaşandığı varsayılan, ancak yaşanmayıp kurulmuş olan hikayelerin incelenmesini sağlayan temel kaynaklı dayanakları bize sunmaktadır. Bu zaman dilimini EBYS içerinde yönetemeyiz. EBYS güncel süreçte belgenin üretilmesi ve erişilmesi bağlamında kendi iç dinamikleri olan ve kullanıcıları tarafından korunma zorunluluğu duyulan bir uygulamamdır. Güncel süreci sonrasında EBYS'deki belgelerin iş süreçlerini yürütenler tarafından değeri ikinci sıraya düşer ve koruma yaklaşımından uzaklaşılarak, unutulmaya yüz tutar. Belgelerin arşivsel süreci belgenin ikinci baharıdır ve farklı yaklaşım ve yöntemlerle yönetilmesini gerektirir.

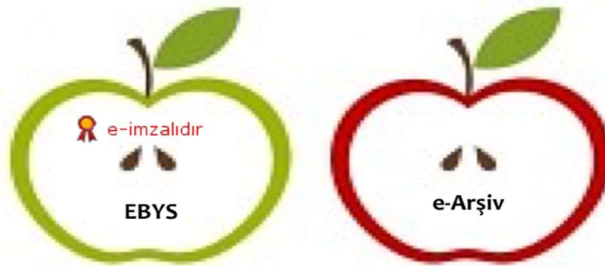
Güncel ve idari fonksiyonunu yitirmiş belge/bilgiyle EBYS uygulamasını meşgul etmeye gerek yoktur. Güncel iş ve işlemlerin daha hızlı, güvenilir ortamlarda yürütülmesi özgürlüğünü kurumlara vermek gerekir. EBYS bunu sağlayan bir platformdur. EBYS belge/bilgi depolama yeri değil, iş üretme, belge üretme sürecinin yönetildiği platformudur. Kurumsal belleği oluşturan belge/bilginin

depolaması ve yönetilmesi ise EBYS uygulamalarıyla entegre çalışabilen kendine özgü dinamikleri olan e-Arşiv Platformunda yapılması gerekir. Bundan 10, 20, 50, 100 yıl sonra kurumunuzu nerede görmek istediğiniz önemlidir. Bir geleceğin olması için bir geçmişin olması gerekir. Deyim yerindeyse "kabarık bir arşiv" vardır. Bu bizi kaygıya sevk etmelidir. Bu kabarık arşiv bizim kurumlarımızın, toplumumuzun, devletimizin geçmişidir. Arşiv belgesi kendisinden başka her şeyi tarihselleştirir ve kendisini tarihin öznesi olarak inşa eder. İşte bu özneyi özenle yönetebilmeliyiz, yüklemi ile buluşturabilmeliyiz.

John Locke'un "insan ancak kendine ait, onu diğerlerinden ayıran geçmişiyle bağlantı kurabildiği ölçüde bireydir" (Boyer, 2015) önermesinde de yer alan klasik felsefi varsayımından yola çıkarak 'kurumlar ancak kendine ait, onu diğerlerinden ayıran geçmişiyle bağlantı kurabildiği ölçüde kurumdur' diyebiliriz. İşte bu noktada kurumsal bellekler devreye girer. Kurumun bir eşi daha olmayan kendi geçmişini, kurumsal belleği (arşivi) oluşturur. Kurumun bu geçmişe erişimi kuruma özgüdür ve eşsizdir. Bilgi-belgenin sığınağı olan arşivler, bilgi-belgeyi tekrar hayatın parçası haline getirmeye çalışan tüketim kültürünün bir parçası olarak yok edilmemelidir.

Kurumsal belleği oluşturan arşivlerin işleyişi pasif bir depolamadan ibaret değildir. Arşiv, kurumsal belleği oluşturan belgeleri/bilgileri aktif bir şekilde yapılandırır, eklemeler ve çıkarmalar yapar, boşlukları uygun materyallerle doldurur. Bu yapılandırma işlevi, belge yönetimi ve arşiv disiplininin yöntem ve tekniklerinin uygulanmasını gerektirir. O halde geliştirmelerde ve uygulamalarda yöntem ve teknikler önemlidir.

Belge yönetimi ve arşiv uygulamaları birbirlerini besleyen süreçlerdir. "Belge Yönetimi" ve "Arşiv" elmanın iki yarısı gibidir. e-Arşiv, EBYS uygulamalarıyla varlık bulmaktadır. Her şeyden önemlisi e-Arşivin temel kaynağı ve varlık nedeni EBYS'lerdir. EBYS yoksa e-arşiv yoktur, ancak bununla da sınırlı değildir. Kurumsal belleği oluşturan diğer kurumsal belge-bilgi varlıklarını da aynı sistem içerisinde ilişkilendirerek barındırır. Bu ilişki dikkate alınmadan kurgulanacak bir kurumsal belleğin sürekliliğinden ve güvenilirliğinden söz etmek mümkün değildir.



Resim-1: EBYS ve e-Arşiv

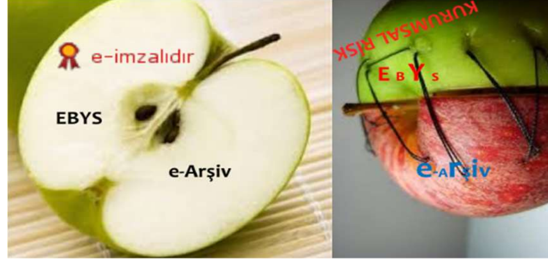
Arşiv belgelerini "kutsal emanet" olmaktan çıkarmak gerekir. Kayıt tutma yöntem ve teknikleri geliştikçe, kurumsal bellekler daha da güçlenmeye başlamıştır. Arşiv belgeleri, kutsal emanetler değil, kurumların DNA'sını barındıran kayıtlarıdır, bir anlamda kurumların arşivleri/kurumsal bellekleri, kurumların DNA'sının gizli olduğu yerlerdir. O halde "kurumların DNA'sı kurumların arşivlerinde gizlidir" diyebiliriz. Çağımızda kurumlar var olabilmek için DNA'sını keşfetmek ve korumak zorundadır. DNA bozulursa, korunamazsa kurumların evrimi ve gelişimi de sağlanamaz. Bu nedenle kurumlar arşivlerine sahip çıkmalıdır. Kurumsal bellekleri oluşturan arşivler kurumların, devletlerin, milletlerin geleceğidir.



Resim-2: Kurumsal Bellek ve Bilginin DNA'sı

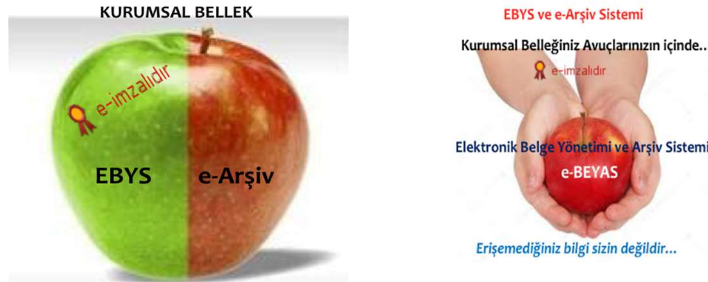
Endüstri 4.0 başlığı altında yapay zeka gibi ileri düzey uygulamalarla insanlığı şekillendirmektedir. Dünya şimdi bilginin DNA'sının peşinde, insanlığın bilgi birikimi bir şekilde yok olursa, bu bilgi birikimine bizi ulaştıracak, bu bilgi birikimini kısa sürede yeniden yaratacak bir DNA oluşturma peşinde, bu yapay zekalar olabilir mi? Artık çok sık duyduğumuz, yaşamımızın içinde olan yapay zeka uygulamaları bu DNA'yı yaratma peşinde… Günümüzün en önemli sorularından birisi: İnsan beyinleri arşivlenebilir mi? Bedenlerimiz olmayabilir ama yapay zeka ile beyinlerimiz yaşayabilir. Kurumlar olmayabilir, ancak kurumların DNA'sı yaşayabilir. Bunu da bilgi sistemleri ve bilişim yönetimi uygulamaları sağlayacaktır.

EBYS, e-Arşiv, yapay zeka, dijital belge gibi yaşamımıza, iş süreçlerimize giren bu kavramlar, kimilerine göre bir kaosun habercisi, kimilerine göre yıllardır köklü çözümler bulunamamış belge-bilgi-arşiv sorununa çözümün habercisidir. Her ikisinin de doğruluk payı vardır. Bu doğruluk, bu sürenin nasıl yönetildiği ile ilgilidir. Günümüzün gerektirdiği yenilikçi bilgi teknolojileri kullanmak gerekliliğin ötesinde bir zorunluluktur. Değişime, gelişime karşı olmak değil, değişimi ve gelişimi yönetebilmek çağımızın başarı sırlarının arasında ilk sırada yer almaktadır.



Resim-3: e-Arşiv ve Kurumsal Risk

Belge yönetimi, arşiv uygulamalarındaki bu yeni düzen bir kaos mu, yoksa bir düzen mi? İyi yönetilemezse kurumlar bir kaos ile karşı karşıya kalacak, iyi yönetilirse düzene gidişin başlangıcı olacaktır. Bu açıdan baktığımızda EBYS'yi aynı zamanda e-arşiv uygulaması olarak değerlendirmek ve kullanmak kaosun ciddi krize dönüşeceğinin göstergesidir.



Resim-4: Elektronik Belge Yönetimi ve Arşiv Sistemi (e-BEYAS)

e-BEYAS, EBYS ve e-Arşiv Sisteminin entegre çalışması üzerine yapılandırılmış bir süreçtir. Kurumsal belleklerimizi geleceğe taşıyabilmek, milli belleğimiz gelecek nesillere aktarabilmek için sistemlerimizi bu temel felsefe ile kurgulamalıyız, yazılımlarımız bu bağlamda geliştirmeliyiz. Kurumsal dinamiklerimiz doğrultusunda gelecekte de var olabilmek için yerli yazılım, yerli sistemler kurmalıyız. Dünyada gelecek artık yenilikçi bilgi teknolojileri üzerinden kurgulanıyor ve yapılandırılıyor. EBYS ve e-Arşiv sistemleri de öncelikli alan içerinde yer almaktadır.

Bu bağlamda çağımızın yenilikçi bilgi teknolojilerinin kullanımı güvenliğe farklı boyut getirmektedir. Çünkü siber saldırılardan zarar gören artık bilgisayarlarımız, donanımlarınız değil, kurumsal belleğinizdir, yani güvenlik ihlaline uğrayan belleğiniz olacaktır. Siber Güvenlik neden önemli, çünkü onlar belleklerinize, beyinlerinize girebilirler. O halde güvenlik her zamankinden daha önemli boyut kazanmaktadır. Bu bağlamda güvenlik; (1) kişiye özgü güvenlik, (2) **kuruma özgü güvenlik,** (3) sisteme özgü güvenlik, (4) **devletlere özgü güvenlik** olarak düşünülmelidir. Açık kamu verisi- açık yönetim gibi yaklaşım ve

uygulamaların gündemde olduğu çağımızda belge yönetimi ve arşiv uygulamaları kendi strateji ve politikalarını, gizliliği, mahremiyeti ve etik çerçevesini ortaya koymalıdır. Arşivlere sahip olmak, sadece bir arşivimiz olsun diye arşiv kurmak yetmez. Büyümek, gelişmek ve dönüşmek için yenilikçi bilgi teknolojilerini kullanmak gerekmektedir.

e-Arşiv Sistemi Pilot Uygulama

Bilgi yöneticileri ile bilişimcilerin birlikte çalışması, alanı ileri götürmek için şart, bu Ankara Üniversitesi'nde deneyimlendi, Ankara Üniversitesi Belge Yönetimi ve Arşiv Sistemi (BEYAS) Koordinatörlüğü, Bilgi İşlem Daire Başkanlığı ve TÜRKSAT ile birlikte çalışarak güzel gelişmeler sağlandı ve e-BEYAS Uygulamasının ilk fazı olan "Elektronik Belge Yönetim Sistemi" hayata geçirildi. Bilginin e-ortamda etkin, güvenilir yönetimi böyle bir işbirliğini gerektiriyordu. Kuşkusuz deneyim varılan yer değil, gidilen yoldur. Bu yolda Ankara Üniversitesi BEYAS Koordinatörlüğü ve Bilgi İşlem Daire Başkanlığı, TÜRKSAT tarafından geliştirilen ArşivNET uygulaması ile e-BEYAS uygulamasının ikinci fazını oluşturan "e-Arşiv Sistemi" konusunda pilot çalışmalarını başlattı, kısa sürede güzel uygulamaların çıkarılması öngörülüyor. Böylece başından beri öngörülen ve ona göre kurgulanan e-BEYAS uygulaması bütünsel bir yapıya kavuşturulacaktır.

Bu kapsamda e-Arşiv platformu görevi yapacak ArşivNET yazılımı arayüzlerinden birkaçını burada verelim;

- Arşiv Malzemesi Tipi Tanımlama/Güncelleme
- Arşiv Malzemesi Tanımlama
- Arşiv Malzemesi Sorgulama
- Değer Tipleri Tanımlama
- Değer Tanımlama
- Varlık Tipleri
- Varlıklar
- Arşiv Planları vb.

Bunlardan birkaçına kısaca değinelim.

Arşivnet Giriş

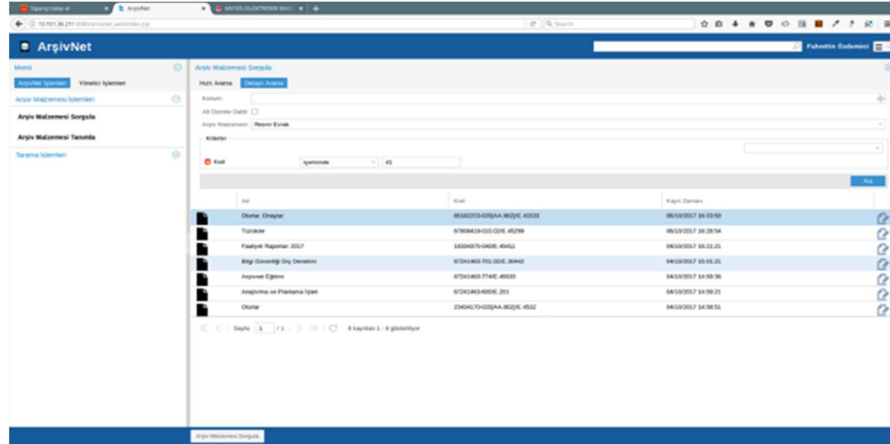
Çağımızın gerektirdiği yenilikçi bilgi teknolojilerini kullanarak kurumsal bellekleri oluşturan arşiv malzemelerinin yönetimini sağlayacak platforma giriş.



Resim-5: Arşivnet Giriş

Arşiv Malzemesi Sorgulama (ArşivNet)

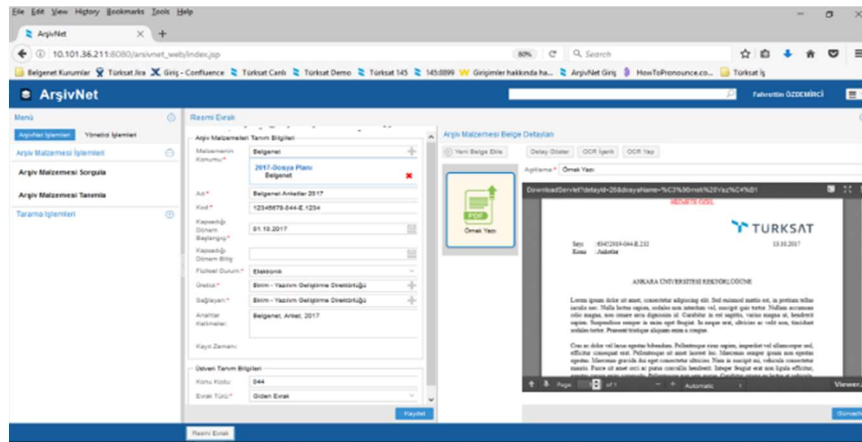
Sorgulama/Arama tüm bilgi sistemlerinde olduğu gibi e-Arşiv uygulamalarında da en önemli fonksiyonlardan birisini oluşturmaktadır.



Resim-6: Arşiv Malzemesi Sorgulama (Arşivnet)

Arşiv Malzemesi Tanımlama – (ArşivNet)

Ne kadar tanımlama, o kadar sorgulama/arama imkanı demektir. e-Arşiv uygulamaları, üstlendiği ve üstleneceği işlevler dikkate alınarak tanımlama ayrıntıları belirlenmelidir.

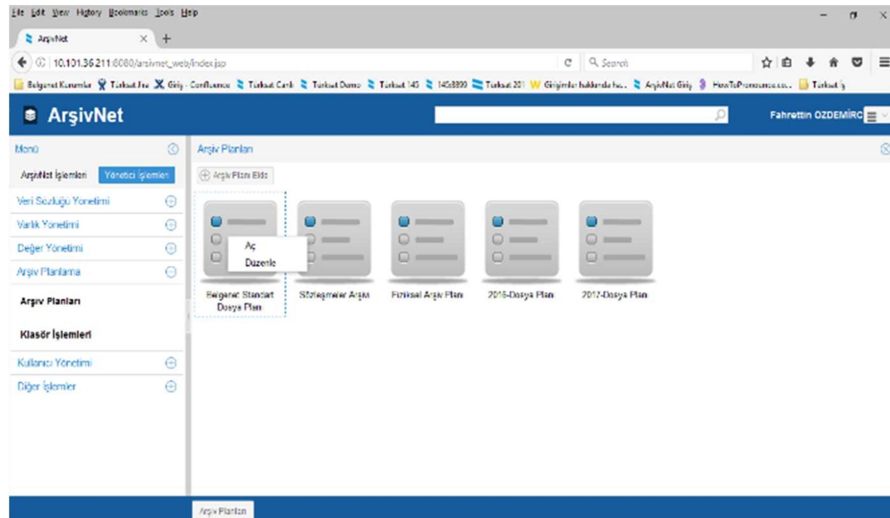


Resim-7: Arşiv Malzemesi Tanımlama (Arşivnet)

Arşiv Planları– (ArşivNet)

Arşiv dosya planları, gereksinim duyulan belge-bilgiye gereksinim duyulduğu anda erişim için kurum ihtiyaçları dikkate alınarak birden çok arşiv dosya planı kullanılabilmelidir.

Bu yaklaşım belgelerin üretim yerleri ile bağını koparmak anlamına gelmemelidir. Bir bilgi sistemi olarak e-Arşiv uygulamasının daha işlevsel kullanılmasını sağlanacaktır.



Resim-8: Arşiv Planları (Arşivnet)

EBYS ve e-Arşiv uygulamaları bir dönemin başlangıcıdır ve bir dönüşümü tanımlamaktadır. Elektronik belge yönetimi ve e-arşiv sistemleri kurumsal belleklerin geleceğini ve geleceğin kurumsal belleklerini şekillendiren uygulamalardır. Onun için bu uygulamaların boyutları iyi belirlenmeli ve doğru kullanılmalı ehil kişilerce yönetilmeli, yönlendirilmelidir. Geleceğin kurumsal bellekleri nereye doğru evriliyorsa, geleceğin belge yöneticileri ve arşivcileri de oraya doğru evrilmeli ve kendini geliştirmelidir. Zira kurumsal bellekleri oluşturan veri-bilgi-belgeler bu sistemlerde üretilmekte, arşivlenmekte ve erişilebilmektedir. Kapsama alanı, etkileri çok geniş ve çok çok uzun soluklu olan bu uygulamaların geliştirilmesinde, yönetilmesinde ve kullanımında bilgi/belge yöneticileri, bilişimciler, bilgisayar mühendisleri, yazılım mühendisleri, yönetim bilimciler birlikte çalışmalıdır. Gelecek için yerli yazılımlar, yerli sistemler geliştirilmeye devam edilmelidir.

Kaynakça

Boyer, Paskal (2015). "Anılar ne işe yarar? Hatırlamanın biliş ve kültürle ilgili işlevi", Zihinde ve kültürde bellek/Yayına hazırlayanlar: Paskal Boyer, James V. Wertsch; çeviren Yonca Aşçı Dalar. İstanbul: T. İş Bankası Kültür Yayınları. İçinde 5-36.ss.

e-Yazışma Projesi, Genelge (2017/21). T.C. Resmi Gazete, (30210), 14 Ekim 2017.

Özdemirci, F. (2017). " Belge ve arşiv yönetiminde yeni ufuklar ve kuramsal yaklaşımlar", Bilgi ve Belge Yönetimi: kuramsal yaklaşımlar / yayına hazırlayanlar: Bülent Yılmaz, Turgay Baş, Semanur Öztemiz, Meltem Dişli. İstanbul: Hiperlink Yayınları. İçinde 219-232. ss.

Özdemirci, F., Bayram, Ö. G., Torunlar, M., Saraç, S. ve Yalçınkaya, B. Elektronik belge yönetimi ve arşivleme sistemi: Geçiş süreci ve uygulama yönetimi. Ankara: 2013.

TS 13298 Elektronik belge ve arşiv yönetim sistemi. Ankara: TSE, 2015.

İngiliz Milli Arşivi'nin Yeni Stratejilerinin Gözden Geçirilmesi: Yenilikçi (Disruptive*) Arşiv Modeli

Yrd. Doç. Dr. Lale ÖZDEMİR

Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Öz

Dijital çağda, bilgiye erişebilme beklentisi hiç olmadığı kadar yüksektir. Bu beklenti, bir bilgi merkezi olarak arşivlerin kullanıcılarına sunduğu hizmetler açısından da geçerlidir. Teknolojik çağda mevcut arşivsel uygulamaların sabit kalması mümkün değildir. Zira, içinde bulunduğumuz teknolojik çağ, bilgi ve belge alanını ve özellikle elektronik belgelerin arşive devri konusunda yenilikler getirmekle birlikte, çok ciddi zorlukları da beraberinde getirmektedir. Elde edilen bilginin benzeri olmayan bir miktarda erişimini yönetmek; erişilmek istenen bilginin keşfinde beklenmedik sonuçlar; erişilen bilgiyi anlamak için yeterli bağlamı sağlamak; erişimi açık ve verilerin çok fazla olduğu bir dünyada mahremiyet, gizlilik ve güvenliği erişim, paylaşma ve yeniden kullanım ile dengelemek; bilgi/belge oluşturanlarının ve tüketicilerin rollerini, sorumluluklarını ve davranışlarını belirlemek bu zorluklardan bazılarıdır (McLeod, 2015, s.4-5). Ayrıca oluşturulan bilginin miktarı açısından dijital buzdağı oldukça büyüktür. Rakamlar, üretilen ve kopyalanan bilginin/verilerin geçen her iki yılda ikiye katlandığını ve 2020'de 44 zettabayta ulaşacağını gösteriyor (McLeod, 2015, 5). Kamu kurum ve kuruluşları bu sayısız yığınlar arasında uzun vadede arşivde saklanacak elektronik belgeleri ayıklayıp değerlendirecektir. Bu belgeleri, milli hafızayı korumak adına elektronik belgenin türünü, formatını göz önünde bulundurmaksızın saklamak arşivlerin görevlerindendir. İngiliz Milli Arşivi'nin geliştirdiği 'Disruptive' Arşiv Modeli işlevselliği bunu yapabilmeyi hedeflemektedir. Bu çalışmanın amacı, elektronik ortamda üretilen belgelerin arşive devri için İngiliz Milli Arşivi'nin yeni geliştirdiği 'Disruptive' Arşiv Modelini incelemektir. 'Disruptive' Arşiv Modeli, mevcut arşivcilik uygulamalarının temelden gözden geçirilmesine dayalı dijital tasarımlı ve sezgisel arşiv olarak tanımlanabilir (The National Archives Digital Strategy, 2017, s.6). Bu çalışmada İngiliz Milli Arşivi'nin yeni arşiv modeli incelenmesiyle birlikte, dijital belgelerin milli arşivlerine devir konusundaki güncel kültürel, teknolojik ve yönetişim sorunlar da ele alınmaktadır.

*Mevcut arşivcilik uygulamalarının temelden gözden geçirilmesine dayalı dijital tasarımlı ve sezgisel arşivdir.

Anahtar sözcükler: *Dijital Arşiv, Elektronık Belge Yönetimi, Arşivsel Uygulamlar, Yenilikçi (Disruptive) Arşiv Modeli*

Giriş

Arşivlerin temel görevi milli hafızayı muhafaza etmektir ancak dijital çağda üretilen belge türü ve miktarının son derece fazla olması bu durumu hiç olmadığı kadar zorlaştırmaktadır. Bu nedenle teknolojik çağda mevcut arşivsel uygulamaların sabit kalması mümkün değildir. İçinde bulunduğumuz teknolojik çağ, bilgi ve belge alanında ve özellikle elektronik belgelerin arşive devri konusunda yenilikler sunmakla birlikte, çok ciddi zorlukları da beraberinde getirmektedir. Günlük hayatı kolaylaştıran teknolojik gelişmeler; mobil cihazların kullanılması, e-devlet uygulamaları üzerinden erişim gibi, kurum ve kuruluşların bilgi ve belge yönetimi süreçlerini ve iş akışlarını da değiştirdiğini söyleyebiliriz. Kurum ve kuruluşlarda elektronik ortamda doğmuş (born digital) bilgi ve belgeler farklı bilgi yönetimi platformlarda üretilmektedir. Örneğin, EBYS ve ortak sürücüler gibi. Ancak kurumlarda üretilen bilgi ve belgelerin sadece EBYS ve ortak sürücülerde yer almadığı unutulmamalıdır. Zira, bilişim teknolojilerinin gelişmesiyle beraber kamu kurumları artık çok çeşitli platformlarda belge niteliği taşıyabilecek bilgi ve belge üretiyorlar. Örnek olarak, sosyal medyada üretilen bilgi, belge niteliği taşıyorsa bunlar ilerleyen dönemde arşiv malzemesi olarak değerlendirilebileceği unutulmamalıdır. Bilginin üretildiği diğer platformlar ise intranetler, e-posta sistemleri, internet olabilir. Kısacası, doğuştan elektronik belgelerin yanı sıra çoklu ortam malzemeleri, ses, video ve yarı yapısal ya da yapısal kaynakların uzun vadede korunup arşive transfer edilmesi gerekebilir (Yalçınkaya, 2016, s.221).

Bu çalışmada, İngiliz Milli Arşivinin geliştirdiği Yenilikçi (Disruptive) Arşiv Modeli incelenmektir. Bu arşiv modelinin örnek alınmasının en başlıca nedeni; İngiltere dışında da uygulanma niteliği olması ve dünya çapında bu türdeki ilk model olmasıdır. Böylece 'Disruptive' Arşiv Modelinin tanımı mevcut arşivcilik uygulamalarının temelden gözden geçirilmesine dayalı dijital tasarımlı ve sezgisel arşiv olmasıyla birlikte, mevcut uygulamaları tamamiyle değiştiren yeni teknolojinin kullanımıyla yürürlüğe girecek bir modeldir (ayrıca bkz. Disruptive technology, Cambridge Business English Dictionary).

Dijital Çağda Değişen Bilgi ve Belge Yönetimi Alanı

Dijital çağda arşivlerin milli hafızayı muhafaza etmelerinin karmaşık ve zor olmasının bir kaç nedeni söz konusudur. Öncelikle bilişim teknolojilerinin gelişmesi ve bilgisayar devrimi olarak adlandırılan bu çağda ortaya çıkan teknoloji kullanımı ve çeşitliliği kurumların bilgi yönetimi anlayışını değiştirmiştir. Bu bağlamda kurumlarda bir e-dönüşüm süreci başlamış ve bu da, hızlı ve etkili bir şekilde kurumsal bilgi ve belge akışına ve kurumsal faaliyetlere yansımıştır (Yalçınkaya ve Özdemir, 2016, s.35). Bununla birlikte kurumsal faaliyetlerde öngörülen bu artan işlevselliğin, bilgiye erişim açısından da beklendiği söylenebilir. Örneğin, 21. Yüzyılın dijital dünyası, arşiv

kullanıcılarının arşivlerdeki geleneksel yazılı rehberlerin yanı sıra, podcast olarak bilinen (internet üzerinden otomatik olarak indirilebilen ve dijital formatta yer alan dijital ses dosyaları) yeni bir tür arşiv yapısını gerektirmektedir. Dijital çağı ne kadar da kapsamlı teknolojik imkanlar sunsa bile, daha önce söz konusu olmayan risklere yol açtığı da söylenebilir. Kamu kurum ve kuruluşlarında olağanüstü boyutlarda veri ve bilgi üretimi, kurumlarda elektronik belgelerin gereksiz yedeklenmesi, erişimin dijital çağda kolaylaştığını fakat bu avantajın aynı zamanda beraberinde ciddi bilgi güvenliği zaaflara neden olduğu ve mahremiyetin dijital çağda daha zor korunduğu bir ortama sebep olmaktadır. Bu konuda arşivleri doğrudan etkileyen diğer konuları şu başlıklar altında sıralayabiliriz:

Bilginin Kurum ve Kuruluşlarda Bir Varlık Olarak Kabul Görmesi

Gelişen teknolojinin sağladığı bilgiye hızlı ve kolay erişim, bilgi yönetimi alanındaki geleneksel yaklaşımların değişimine neden olmuştur. Bir çok ülkede arşivcilik mevzuatın var olması ve vatandaşın resmi bilgiye erişimini kolaylaştıran Bilgi Edinme Hakkı kanunları kapsamında kamu kurumlarının ürettiği bilgi, arşiv kullanıcılarına sunulan hizmetler yeni boyutlara ulaşmıştır. Uluslararası koşullarda bilginin başlı başına bir varlık olarak görülmesi ve halkın bilgiye erişim hakkı yeni çağda üzerinde tartışılan konular arasındadır. Örneğin, EBYS'de saklı belirli bir proje ile alakalı belgeler gibi, bir bilgi varlığı; Bilgi varlığı, tek bir birim olarak tanımlanabilen ve yönetilebilen, dolayısıyla anlaşılabilir, paylaşılabilir, korunabilir ve etkili biçimde kullanılabilir olan bilgi bütünüdür. (What is an information Asset, The National Archives, 2017). Fiziksel belgelerden farklı olarak, elektronik bilginin üretildiği andan itibaren yönetilmesi gerekmektedir. Aksi takdirde bu belgeler, eğer ileride milli hafıza açısından değerli olup arşive transfer edileceklerse, bu mümkün olmayabilir. Elektronik bilgi yönetiminin ilk ve kritik aşaması bilginin bir varlık olarak tanımlanıp kabul edilmesidir. Kurumlar bilgiyi başlı başına bir varlık olarak görmezlerse o bilginin sürdürebilirliğinin sağlanması nerdeyse imkansızdır. Kurumlarda her birimin bilgi varlıklarını kayıt altında aldığı bir dosya yolu, isim, hassasiyet, saklama süresi, varlık sorumlusu gibi bilgilerin olduğu bir envantere sahip olması gerekir. En önemlisi, bilgi varlıklarının belgelendirilmesi olası bir bilgı güvenlik vakasında, belgelerin bütünlüğü, erişebilirliği ve gizliliği açısından hayati nitelikte olacaktır. Ancak bilginin gerçek bir varlık olarak kabul edilebilmesi için milli arşivler ve kamu kurumlarının bu konuda önderlik yapmaları gerekmektedir. Örneğin, 2007 yılında İngiltere Başbakanı Gordon Brown özgürlük ve yeni bir takım yasal düzenlemeler üzerine yaptığı konuşmasında; kurum ve kuruluşların ürettiği bilginin bir varlık olduğunu, hassasiyetini yitirmiş bilginin kamuoyuyla paylaşılmasını ama bunu yaparken vatandaşın mahremiyetinin korunması gerektiğini vurgulamıştır (Gordon Brown, Speech on Liberty, 2007).

Dijital Süreklilik

Kamu kurum ve kuruluşları zamanı gelince ilgili mevzuat ya da yönetmelikler doğrultusunda elektronik belge devredeceklerse bilginin üretildiği andan itibaren dijital sürekliliğin uygulanması şarttır. Dijital süreklilik kurumsal faaliyetlerin gerçekleşebilmesi için gerekli olan bilgiyi korur. Dijital süreklilik; kurumların ihtiyaç duydukları sürece, elektronik bilgiyi istedikleri şekilde kullanma kabiliyetidir. Bu kullanma kabiliyeti de şu işlemlerden ibarettir: Bilgiye ihtiyacı duyulduğunda, onu bulabilmek, açabilmek, istediği şekilde kullanabilmek, ne olduğunu anlamak ve neyin hakkında olduğunu bilmek ve son olarak da, bilginin bütünlüğüne güvenebilmektir (Digital Continuity, The National Archives). Dijital süreklilik tam olarak anlaşılamadığında uygulamada bilgi yönetimi süreçleri de kolay olmayabilir. Dijital süreklilik, sadece teknolojinin kullanılmasından ibaret değildir. Bundan ziyade, kapsamlı ve iyi yönetilen kurumsal bilgi yönetiminin uygulanmasıyla gerçekleşebilir. Dijital süreklilik uygulanmadığında uzun vadede bilgi uygun bir şekilde imha edilemez, gerekli olduğunda yeni teknolojilere göç edilemez, kullanılmayan formatlarda açılamaz olur ve böylece bilginin bütünlüğü zedelenir. Elektronik belgeler sağlıklı bir şekilde arşive devredilecekse, kurumların bilgi yönetimi doğrultusunda; uzun vadede sürdürebilirliği olan formatlarda belge üretmeleri gerekmektedir. Bununla birlikte DROID gibi profil belirleme araçların kullanılması, düzenli olarak bilgi varlıkların olasılık risklerin (belli formatların zamanla kullanılmaması ya da bilgiye izinsiz erişim gibi) doğrultusunda değerlendirilmesi ve mutlaka kurumun yönetimine Kıdemlı Bilgi Sorumlusunu atanması şarttır.

Elektronik Belgelerin Arşivlenmesine Yönelik Yaklaşımlar

Dünya çapında elektronik belgelerin transferi için gerekli teknolojik altyapıya sahip milli arşivler sayılıdır. Elektronik belgelerin transferi için gerekli olan depolama ya da veri ambar sistemi bulunmamaktadır. Bunun sebebi ise arşivlerin yüzyıllar öncesi fiziksel belgelerinin devri ve uzun vadede saklanması üzerine kurulmuş olmalarıdır. Elektronik belgelerin arşivlenmesi konusunda önderlik yapan İngiliz Milli Arşivi (The National Archives) yıllardır bir dijital arşive sahiptir. Arşivin Dijital Belge Altyapısı çok büyük boyutlarda (bir çok petabyte) ilişkili üst veriyle birlikte esnek bir yaklaşım içerisinde güvenilir ve etkin bir şekilde koruma gerçekleştirir (Digital Strategy, The National Archives, 2017, s.5). İngiliz Milli Arşivinin hedeflerine göre arşivcilik mevzuatı yükümlülüklerine uymak için (The Public Records Act, 1967), 2017 yılında 18 kurumun doğuştan elektronik belge transferi gerçekleştirmesi bekleniyor. Elektronik belge transferi gerçekleştirmesi beklenen kurum sayısı sırayla şöyledir; 2018 yılında 21 kurum, 2019 yılında 22 kurum, 2020 yılında 32 kurum ve 2021 yılından itibaren 50 kurum (The digital landscape in government 2014-15, The National Archives, 2016, s.6).

Bu konuda göstermiş olduğu başarıya rağmen, İngiliz Milli Arşivi hala birinci nesil dijital arşiv olarak tanımlanıyor. Bir birinci nesil arşivin arşivsel süreçleri fiziksel belgeler üzerine kurulmuştur. Arşivin birinci nesil arşiv olarak tanımlanma sebebi, arşive transfer edilecek elektronik belgelerin hala fiziksel belgelerin yaşam döngüsüne uygun bir şekilde ayıklama ve değerlendirme gibi arşivsel süreçlerde gerçekleşmesindendir. Transfer sonrası elektronik belgeler, tıpkı fiziksel belgeler gibi, uluslararası kataloglama standartlara göre tanımlanır ve katalog doğrultusunda arama ve erişim gerçekleştirilir (The National Archives Digital Strategy, 2017, s.6). Arşivin halihazırda uyguladığı dijital transfer süreci fiziksel belgeler için kullanılan yöntemleri takip etmekle birlikte, kapsamlı müdahale gerektirmektedir. Elektronik belge transferi için kullanılan teknoloji önemli ölçüde fiziksel transfer için uygulanan süreçleri taklit etmektedir. Örneğin, ‘bir doküman’ oluşturmaya izin veren program söz konusudur ve bu doküman ‘dosya planında’ yer alan bir ‘dosyaya’ konulacaktır. Ancak yeni teknolojilerin hızlı geliştiği bir dönemde, bir hızlı iletinin (instant messaging) ya da Trello gibi bir proje yönetim sisteminin analog muadili bulunmamaktadır (The generation game: evolving with the digital record, The National Archives).

Yenilikçi (Disruptive) Arşiv Modeli Üzerine

İngiliz Milli Arşivi Yenilikçi Arşiv Modelini anlatan 2017-19 Dijital Strateji belgesini Mart 2017’de yayınladı. Bu model, dünyada ilk olup mevcut arşivsel uygulamalarının temelden gözden geçirilmesine dayalı dijital tasarımlı ve sezgisel arşiv üzerine kuruludur. Dijital ortamdaki elektronik belgeler 0 ve 1’den ibaret olan bitlerden oluştuğu için, bir dijital transfer altyapısı bu bitleri koruyarak o belgelerin ya da verinin uzun vadedeki korumasını sağlayabilir. İngiliz Milli Arşivinin geliştirdiği Yenilikçi Arşiv Modeli ikinci nesil dijital arşiv kavramına dayanmaktadır. İkinci nesil arşiv, birinci nesil arşivden daha esnek bir yaklaşıma sahip olup dijital yapıları türe, format ve arşive transfer edildikleri zaman ki durumlarına bakmaksızın devralır. Bu yeni modelin geliştirilmesinin başlıca gerekçelerinden biri, gelecekteki elektronik belgelerin bugün gördüğümüzden çok daha farklı olma olasılığıdır. Örneğin, devlet düzeyinde alınan ve milli hafıza için önemli olan bazı kararlar bir yazılımın farklı versiyonlarında şifrelenmiş olabilir. Alınan kararların belgelenmesi, kodlamayı yazan yazılımcının şekil vermesiyle ortaya çıkabilir (The generation game: evolving with the digital record, The National Archives). Bu Yenilikçi (Disruptive) Arşiv Modeli henüz yürürlüğe girmemiştir ancak 2019 yılında yürürlüğe girmesi planlanmaktadır. Çok iddiali olan bu model, farklı medya içeriğinin kanıtsal değer taşıdığını varsaymaktadır. Bunların arasında websiteleri, veritabanları, datasetler ve bilgisayar programları yer alırken, bu model bunları değerlendirilip korumayı hedeflemektedir. Aynı zamanda yenilikçi arşiv yaklaşımı dijital bilginin kümeleşmiş (aggregate) halde tarihi değer taşıyabileceğini de öngörmektedir (Creating the disruptive digital archive, Digital Preservation Coalition).

Bir ikinci nesil arşiv olarak, Yenilikçi Arşiv Modeli mevcut arşivcilik prensiplerin temelden gözden geçirilmesini sağladığı için birinci nesil arşivden aşağıdaki hususlarda farklı ve yenilikçi olarak değerlendirilebilir:

- ‘Disruptive’ arşiv kamu kurum ve kuruluşları tarafından üretilen formatlara bakmaksızın tüm dijital belgeleri devralır,
- Kullanıcılara farklı zamanlarda farklı değer kategorileri sunan net olan bir değer planı mevcuttur,
- Yeni sistemler hakkındaki tartışmalara katkı sağlar, böylece dijital koruma sorunları erken ele alınır,
- Bağlam sağlamak ve risk yönetimi için yeni yöntemlerin geliştirilmesi ve belgelerin bütünlüğünün korunduğuna dair güvence verir,
- Belgeleri üretildiği andan itibaren arşivsel malzeme olarak kabul eden yaşam döngüsü modeline dayanan yaklaşımları uygular ve belgelerin hep değişim halinde olduğunu kabul eder,
- Büyük boyutlu veri analizi yapıldığı çağda, dijital belgelerin yığın halindeki koleksiyonlarının da değerli olduğunu kabul etmektedir (The National Archives Digital Strategy, 2017, s.6).

Yenilikçi Dijital Arşivin Değerlendirmesi

Mevcut arşivsel uygulamalarının temelden gözden geçirilmesine dayalı dijital tasarımlı ve sezgisel arşiv olması hedeflenen ‘Disruptive’ arşivin temelinde dijital çağda üretilen belgeleri bir kalıba sokmadan sorgusuz bir şekilde kabul etme yaklaşımı söz konusudur. İngiliz Milli Arşivi bu yeni arşiv modelinin 2017-2019 yılları arasında geliştirileceğini ve dört madde doğrultusunda kullanıcılarına ve elektronik belge transfer edecek kamu kurum ve kuruluşlara değer katacağını iddia etmektedir:

Koruma (Preservation)

Arşivler milli hafıza açısından değerli olan belgeleri saklamakla ve bu belgelere erişim sağlamakla topluma değer katarlar. Koruma başlığı altında İngiliz Milli Arşivi ‘Disruptive’ Arşiv Modelinin devir alabileceği belge türlerini çeşitlendireceğini açıklamıştır. Halihazırda birinci nesil dijital arşiv olarak İngiliz Milli Arşivi elektronik belge transferleri görseller, doküman formatları (Word ya da Excel gibi) ve karışık medya (websiteler ve tweetler) belgeleri üzerinde yoğunlaşmaktadır. Ancak söz konusu arşiv; yapılandırılmış datasetleri (structured databases) ve bilgisayar kodu transfer etme yeteneğini geliştirmesi gerektiğini vurgulamaktadır. Arşiv, bunu hayata geçirmek için de yazılım şirketleriyle ve yazılımcı toplumlarla sıkı işbirliği içerisinde olacağını da belirtmektedir. Aynı zamanda korumanın kamu kurum ve kuruluşlarında belgenin üretildiği andan itibaren başlaması gerektiğini ve bu çercevede yeni sistemlere geçecek olan

kurumlara, DROID (profil belirme aracı) gibi konularda destek vermeye devam edeceğini de ifade etmektedir (The National Archives Digital Strategy, 2017, s.7).

Bağlamlaştırmak (Contextualise)

Bu başlık adı altında Milli Arşiv, dijital belgelerin tanımlanma ve bağlamlaştırma konusunun tamamiyle gözden geçirilmesi gerektiği görüşündedir. Bağlamsal tanımlamanın alanda yeni olduğunu ve bunun üzerinde çalışmalar yapılması gerektiğini ve dijital belgelerin birbirine bağlamlaştırdığını ve bağlamsal tanımlamanın çok değişken bir kavram olduğu vurgulanmaktadır. Dijital çağdaki 'Disruptive' teknoloji dünyasında belge tanımlarının değişken olduğu ve sabit olmadığı belirtilmektedir (The National Archives Digital Strategy, 2017, s.9). Aynı zamanda bu başlık altında arşiv, kamu kurum ve kuruluşları üzerindeki iş yükünü hafifletmeyi planlamaktadır. Sadece uzun vadede korunacak belgelerin üst verisinin (referans, provenans, erişim şartları gibi) belge düzeyinde olması ve belge düzeyindeki üst verinin de otomatik olarak sistem tarafından üretilmesi gerektiği belirtilmektedir.

Görüntüleme (Present)

Görüntüleme adı altında arşiv; yeni dijital stratejiyle birlikte, dijital belgeleri web de görüntülemek için yeni bir görüntüleme sistemini geliştirmeye ihtiyaç duyduğunu açıkladı. Bu yeni görüntüleme sisteminin kullanıcı ihtiyacı doğrultusunda geliştirileceğini ve farklı belge türlerini görüntüleme yeteneğine sahip olması gerektiği vurgulanmıştır Örneğin, eposta ve çoklu medya konusunda görüntüleme kapasitesinin etkin olması lazımdır. Yeni sistemin açık uygulama programlama arayüzüne (API) sahip olması planlanmaktadır ve bunun kullanıcılar, yazılımcılar ve donanım açısından şart olduğu görüşü söz konusudur (The National Archives Digital Strategy, 2017, s.10).

Kullanımı Etkinleştirme (Enable Use)

Bu başlık altında Miili Arşivinin yenilikçi planların arasında koleksiyonların bulut'da (cloud) da yedeklenmesi ve böylece arşivin ya da bulut bilişiminden faydalanan araştırmacıların da koleksiyonları bu şekilde işleyebilme imkanına sahip olacakları ifadesi yer almaktadır.

Sonuç

İngiliz Milli Arşivinin 2019 yılından itibaren yürürlüğe koymayı planladığı Yenilikçi Arşiv Modeli çok iddialı olmakla birlikte eğer gerçekleşirse uluslararası alanda elektronik belgelerin transferi için teknolojik altyapısı olmayan arşivlere

önderlik yapabilecektir. Bu modeli uygulamakla, İngiliz Milli Arşivi milli arşivlerin bulunduğumuz dijital çağa uyması gerektiğini hatırlatmakla beraber bunun ancak değişim yönetimi çerçevesinde mümkün olabileceğini vurgulamak gerekir.

Bu yeni arşiv modelinin de riskleri mevcuttur. Öncelikle, İngiliz Milli Arşivi kısa bir sürede belli sorunları aşmak zorundadır. Aşılması gereken sorun, sadece İngiliz Milli Arşivi için değil, tüm milli arşivler için önem arz etmektedir. İngiltere halihazırda 'dijital' yetkinliklere sahip personel bulma sıkıntısı yaşamakta ve özellikle yeni teknolojiler geliştirebilecek ve uygulayabilecek uzmanların arşivler tarafından istihdam edilmeleri gerekmektedir (The National Archives Digital Strategy, 2017, s.5). Diğer bir sorun ise dijital çağda arşivcilik prensiplerinin ve uygulamalarının değiştigi konusundaki algı ve yaklaşım ile alakalıdır. Fiziksel belgelere uygulanan arşivsel süreçlerin dijital belgeler için farklı olduğunun kabul etmek gerekir. Kurumlarda yapılan fiziksel belgelerin ayıklama, değerlendirme ve hassasiyet kontrolü çoğunlukla uzmanlar tarafından manuel olarak yapılmaktadır. Ancak dijital çağda çok büyük boyutlarda farklı sistemlerde, yapısal olan ya da yapısal olmayan bilginin arşivsel süreçlerinin sadece manuel yapılmasının zamanla mümkün olmadığı görülecektir. Bu süreçlerde teknolojiden yardım almak şart olmakla birlikte uzmanların bu işlemleri yaparken veri madenciliği ya da metin madenciliği yazılımlarını kullanması normal hale gelecektir.

Başka bir husus ise kullanıcı beklentileriyle alakalıdır. Dijital çağda elektronik belgelerin arşive transfer edilmesiyle yeni bir kullancı kitlesi ortaya çıkacaktır. Klasik anlamda belgeleri saklamak ve erişim sağlamak yeterli olamayacaktır. Dijital belgelerin veri kullanıcıları olacaktır ve bu kullanıcılar belgeler üzerine bilgisayar kodu (yazılım) yazmak ve çalıştırmak isteyebilirler (The National Archives Digital Strategy, 2017, s.4). Arşivlerin de bir yandan veriyi koruma yükümlülüğünün olmasının yanında diğer yandan da ileride veri kullanım etkinleşmesini sağlamakla sorumlu olacakları için, bu konuda sıkıntılar yaşanması öngörülmektedir.

Son olarak da dijital korumanın zor olmasından dolayı, kesin ve kalıcı çözümler söz konusu değildir. Milli arşivler ve kamu kurumlarının daha pragmatik çözümleri kabul etme konusunda daha esnek olmaları gerekmektedir. Dijital belgelerin korumasında olmazsa olmaz unsurlardan birisi; bitlerin saklanmasıdır. Zira, dijital belgeler için uygun uzun vadeli depolama ortamı bulunmamaktadır. Elektronik belge transferi için gerekli altyapıya sahip olmayan arşivler geçici çözümler uygulayabilirler. Buna; kurumların transfer etme süresi geldiğinde belgeleri bir sisteme alınması (ingest etme) ve daha sonra arşivleme sürecinin tamamlanması örnek olarak verilebilir. Böylece milli hafızanın zarar görmesi engellenmiş olacaktır.

Kaynakça

Creating the disruptive digital archive, Digital Preservation Coalition, (1 Mart) 2017. http://dpconline.org/blog/disruptive-digital-archive adresinden erişildi.

Digital Continuity (resmi website), The National Archives, 1 Eylül 2017 tarihinde http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/what-is-digital-continuity/ adresinden erişildi.

Digital Strategy 2017-2019, The National Archives (2017), 2 Eylül 2017 tarihinde https://www.nationalarchives.gov.uk/documents/the-national-archives-digital-strategy-2017-19.pdf adresinden erişildi.

Disruptive Technology, Cambridge Business English Dictionary (2011). 1 Eylül 2017 tarihinde http://dictionary.cambridge.org/dictionary/english/disruptive-technology adresinden erişildi.

Gordon Brown's speech, The Guardian (27 Şubat 2007). 22 Ağustos 2017 tarihinde https://www.theguardian.com/politics/2007/feb/27/immigrationpolicy.race adresinden erişildi.

McLeod, Julie (2015) Access to information: Challenges and opportunities for the records profession. In: *7th Conference on Scientific Archives*, 24 - 26 June 2015, (s. 1-20). Rio de Janeiro.

The National Archives, The digital landscape in government 2014-15: Business intelligence review (2016). 15 Ağustos 2017 tarihinde http://www.nationalarchives.gov.uk/documents/digital-landscape-in-government-2014-15.pdf adresinden erişildi.

The National Archives, The generation game: evolving with the digital record (21 Eylül 2017). 1 Ekim 2017 tarihinde http://blog.nationalarchives.gov.uk/blog/generation-game-evolving-cope-digital-record/ adresinden erişildi.

The Public Records Act, 1967, 3 Aralık 2017 tarihinde http://www.legislation.gov.uk/ukpga/1967/44 adresinden erişildi.

What is an information Asset, The National Archives (2017). 1 Eylül 2017 tarihinde http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf adresinden erişildi.

Yalçınkaya, B., (2016). E Arşiv Uygulamalarında Teknolojik ve Altyapı Kapsamında Yaklaşımlar Güvenilir E Arşivleme Koşulları Yol Haritası, *e-BEYAS 2015 Sempozyumu: Kurumsal Belleklerin Geleceği*, 21-22 Ekim 2015, (s.221-233). Gölbaşı-Ankara.

Yalçınkaya, B., Özdemir. L. (2016). Elektronik Belge Yönetim Sistemlerinin Kurum ve Kuruluşlarda Değişim ve Dönüşümüne İlişkin Bir Değerlendirme*, ÜNAK 2013 Konferansı: Bilgi Sistemleri, Platformlar, Mimariler ve Teknolojiler*.19-21 Eylül 2013, (s. 121-127). Marmara Üniversitesi, İstanbul.

EBYS (e-BEYAS) ve e-Arşiv Sistemlerinde/Uygulamalarında Yapay Zekâ Yaklaşımı

Dr. Mehmet Altay ÜNAL
Ankara Üniversitesi Fizik Mühendisliği Bölümü

Prof. Dr. Fahrettin ÖZDEMİRCİ
Ankara Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Öz

Yapay zekâ (Artificial Intelligence - AI) makinelerin, insanların öğrenme süreçlerini taklit edecek şekilde programlanması temeline dayanır. Sistem, dış verilerden yararlanarak bir tecrübe süreci geçirdikten sonra öğrenme sürecini tamamlar. Öğrenme sürecini tamamlamış sistemler farklı boyuttaki parametreleri değerlendirerek karar süreçlerine katılırlar. Bu davranış biçimi, insanın yaşam boyu tecrübe kazanarak git gide daha doğru karar verebilme kapasitesinin artmasına benzemektedir. Büyük alışveriş siteleri müşterilerine onların ilgisini çekebilecek ürünleri göstermek ya da sosyal medya hesapları kullanıcıların fotoğraflarını tanımak için yapay zekâ algoritmaları kullanırlar. Amazon, Google, facebook gibi uluslararası büyük internet şirketlerinin bu alanda büyük yatırımlar yapması yapay zekanın giderek artan bir ivmeyle hayatımızda yer alacağının bir işareti olarak görülebilir. Elektronik belge akışı sırasında ortaya çıkan büyük verinin analiz edilerek, sistemin tıkandığı yerler, kullanıcı hataları vb. gibi etkenler AI algoritmaları ile ayrıntılı olarak analiz edilecektir. Algoritmaların sistemin olağan akış sürecinin öğrenmesi sağlanarak ortaya çıkabilecek sorunlar çok önceden belirlenebilecektir. Bununla birlikte anomalilerin önceden tespiti de mümkün olacak, doğabilecek güvenlik açıkları da önceden kestirilebilecektir.

Anahtar Sözcükler: *Yapay Zekâ, Makina Öğrenmesi, Yapay Zekâ Algoritmaları.*

Giriş

Kapitalist ekonomilerde, yapılan bir işin değerli olup olmadığı ekonomik büyümenin gelişimine yaptığı katkı ile ölçülür. Bu nedenle, büyük sermayenin geleceğe yönelik yatırım planları ve son yıllarda yaptığı yatırımların karakteristiği o işin değerinin belirlenmesinde büyük rol oynar. Bu açıdan bakıldığında, Amazon.com, Facebook ve Google gibi büyük sermayeli uluslararası şirketlerin AI alanında yaptıkları yatırımlar son yıllarda giderek artmaktadır. Bloomberg'in C.B. Insights raporlarına dayanarak yapmış olduğu araştırmaya göre, AI

yatırımlarının 2020 yılında %60 büyüme göstereceği tahmin edilmektedir ("A new era," 2017). Bu tahminle birlikte Tactica'nın hazırlamış olduğu rapor göz önüne alındığında 2025 yılına vardığımızda toplam AI pazarının 16 milyar USD büyüklüğünde bir pastaya sahip olacağını söyleyebiliriz (KAUL & WHEELOCK, 2016). Hem Pazar hem de yatırım olarak oldukça büyük bir boyuta ulaşmış AI kavramına uzak kalmak, sadece bu iki ekonomik göstergeye göre bile neredeyse imkansızdır.

Yapay Zekâ ve Bilgi-Belge Yönetimi

AI, çok basit olarak bilgisayarların ya da makinelerin "öğrenme süreçlerine" sahip olmaları sonucunda kazandıkları bir yetenek olarak açıklanabilir. Oluşturulan farklı bilgisayar algoritmaları ile bu öğrenme süreçleri tanımlanmakta, oluşturulan sistem tecrübelerini bir öğrenme sürecinden sonra kullanabilmektedir. Bu algoritmaların yapabildikleri şu an bile o kadar etkileyicidir ki eski Google çalışanlarından Anthony Levandowski, kuralları bir AI algoritması tarafından oluşturulan yeni bir din kurmuştur (Solon, 2017). 7-9 Temmuz 2017 tarihleri arasında, Birleşmiş Milletler himayesinde düzenlenen AI zirvesi, yapay zekanın; fakirlik, açlık, sağlık, eğitim ve çevre sorunları başta olmak üzere çeşitli alanlarda çözüm üretebileceğini vurgulamaktadır ("AI for Good Global Summit," 2017). AI konulu bir zirvenin, doğrudan Birleşmiş Milletlerin himayesinde gerçekleştirilmesi konunun ciddiyeti ve gelecek perspektifi açısından ilgi çekicidir. Bununla birlikte, çağımızın yaşayan en büyük fizikçisi Stephan Hawking'in AI'nin insanlığın sonunu getireceği yönündeki açıklaması madalyonun bir diğer yüzünün oluşturan belki de en büyük katmandır (Cellan-Jones, 2014). Bu distopyanın en büyük paydaşı ise Tesla firmasının sahibi Elon Musk'tır; AI araştırmalarının insanlığı büyük bir felakete sürükleyeceğini bu nedenle de milyar dolarlar mertebesindeki bir bütçeyi, insanlığın AI'den korunması için harcayabileceğini söylemiştir (DOWD, 2017). Kuşkusuz bu iki felaket senaryosu, öne sürenlerin kimlikleri düşünüldüğünde ciddiyetle ele alınması gereken değerdedir.

Sosyal medyadan büyük veri analizine, arama motorlarından akıllı telefonlara kadar hemen her yerde uygulama alanına sahip olan AI'nin elektronik bilgi ve belge yönetimi alanında da kendisine yer bulması elbette kaçınılmazdır. İnsanoğlu mağara duvarlarına resim yaptığından beri bilgiyi saklayıp bir sonraki kuşağa aktarabilme yeteneğini geliştirmeye devam etmektedir. Bilginin en basitinden en karmaşığına kadar tartışılmaz bir değere sahip olduğu büyük keşifler ve imparatorluklar zamanında da biliniyordu. Hatta öyle ki; İngiliz kaşiflerin Hindistan'ı işgali sırasına onlarca bilim insanı Hindistan'ın bitki örtüsünü, jeolojik özelliklerini ve demografik yapısını incelemek için görevlendirilmiştir. İngiliz imparatorluğunun, Hindistan'ın nüfusuna göre sayıca oldukça az olan

askeri gücüyle uzun yıllar boyunca Hindistan'ı yönetebilmesinde sahip olduğu "bilginin" rolü tartışmasız çok önemlidir (Harari & Genç, 2016). 20. Yüzyıl yarıiletken teknolojisinin ilerlemesine paralel olarak bilgisayarların giderek daha yüksek kapasiteye sahip olmasına ve bu gelişmelerin ışığında hayatımızın hemen hemen her alanında kullanılmasına şahitlik etmiştir. Bu süre zarfında bilgi ve belgeler değişik biçimlerde bu dijital dünyada varolmuşlardır. İnternetin yaygınlaşması ile birlikte bilgiye erişimin değeriyle birlikte bilginin petrolden sonraki en büyük güç olduğu da daha iyi anlaşılmıştır. Bu nedenle çok sayıda yazılım, algoritma ve bilişim sistemi bu bilgilere erişilmesi, bu bilgilerin yorumlanması ve anlamlı hale getirilmesi için geliştirilmiştir. 21. Yüzyılın ise bilgi ve belge yönetimi konusunda AI ile birlikte bir üst seviyeye geçeceği, bilginin yorumlanmasının şekil değiştireceği şimdiden değerlendirilmeye başlanmıştır; bilgi ve belge yönetimi alanı için AI uygulamaları geliştiren şirketler de Pazar da boy göstermeye başlamıştır ("Fireman & Co. – A legal industry-focused management consulting firm,"). Bu üst seviye; belgelerin otomatik olarak analiz edilip sınıflandırılması (Ankara Üniversitesi örneğinde senato kararları ile yönetim kurulu kararlarının tanınması ve sınıflandırılması) belge içeriğine göre karar süreçlerinin işletilmesiyle birlikte ses ve el yazısının tanımlanmasını içermektedir (Neururer, 2015). Bir hukuk firması ele alındığında, dava dosyalarının değerlendirilmesi, benzer dava tutanaklarının analiz edilerek çıkabilecek kararın önceden tahmin edilebilmesi belki de yakın zamanda mümkün olabilecektir (Wyatt & Ryan, 2017).

Belge Yönetimi ve Arşiv Alanına Yenilikçi Bilgi Teknolojileri Yaklaşımı

Bilginin üretimi, depolanması, analizi, kullanımı çağımızın yenilikçi bilgi teknolojilerini gerektirdiğine göre belge yönetimi ve arşiv alanında da yenilikçi teknolojiler kullanılmak zorundadır. "Belge merkezleri ve arşivler, geleceğin 'Veri Merkezleri'dir. Artık 'Kurum Arşivi' olmayacak, 'Kurum Veri Merkezi' olacak, bu veri merkezlerinde biz belgeyi nasıl yönetiriz. Sanırım üzerinde durulması gereken önemli hususlardan birisi de budur. Yeni ufuklar, yeni kuramsal yaklaşımlar gerektirir" (Özdemirci, 2017, 229.s.). Yenilikçi teknolojilerin beraberinde getirdiği riskleri olacaktır. Risk ve tehditleri avantaja dönüştürmek için çalışmaların yürütülmesi gerekiyor. Bunu başaramazsak işte o zaman risk ve tehditler bizim kâbusumuz olacaktır. Risk var diye yenilikçi teknolojileri alanımızda kullanmaktan uzak duramayız, riski yönetebilmeliyiz. Birçok disiplinde olduğu gibi, belge yönetimi ve arşiv alanı da yenilikçi bilgi teknolojilerinin etkisi altınadır. Geleceğin belge yöneticileri ve arşivcileri, teknolojiyi bilen, kullanan kişiler olacaktır. Belge yöneticisi ve arşivci evrilmek

zorundadır, yoksa mesleğini robotik sistemlere bırakmak zorunda kalacaktır. Belge yönetici ve arşivcicin şu anda yaptığı işlerin % 70'den fazlasını robotik sistemlere bırakacağı konusunda emareler bulunmaktadır. Yapay zeka ve robotik sistemlerin işsizliği artırıp artırmayacağı konusu tartışılmaktadır. Bu bağlamda uzun vadede insanlığın geleceği için şimdiden neler yapabileceğine ilişkin, Oxford Üniversitesi İnsanlığın Geleceği Enstitüsü (Future of Humanity Institute) disiplinlerarası araştırmalar yürütmektedir (Future Humanity…, 2017). Bu kapsamda "İşimi Robotlar Alacak mı? (Will Robots Take My Job?) https://willrobotstakemyjob.com adresli web sitesi, Arşivcilerin %76'sı, Dosya Görevlilerinin %97'si, Kütüphanecilerin % 65'i mevcut işlerini yapay zeka ve robotik sistemlere bırakacağına ilişkin veriler sunmaktadır (Will Robots…,2017).

Bunun yanında iyimser yaklaşımlar içeren değerlendirmeler de yapılmaktadır. "Yapay Zekâ, insan güvenliğiyle ilgili bir dizi soruna gerçek zamanlı, maliyet etkin ve etkili yanıtlar verilmesinin potansiyel yollarından birisidir. Yapay Zekâ'nın araştırma, sınıflandırma ve yeni modellerinin tespit edilmesine dair uygulamaları, farklı kaynaklardan anlam ve içeriğin ilişkilendirilip ortaya çıkarılmasına yardımcı olabilir. (…) Yapay Zekâ insanların yetkilerini elinden aldığı gibi onları güçlendirir de. Dolayısıyla, Yapay Zekâ sistemlerinin kurulumu ve konuşlandırılmasını yönlendirmek için etik ilkelerin kullanılması gerekir. İnsan güvenliği, çok sınırlı sayıda bir elit kesim için değildir. (…) Bununla birlikte, Yapay Zekâ'nın her derde deva olmadığını da belirtmek gerekiyor. (…) Kısacası, insan güvenliğini mümkün kılan Yapay Zekâ, doğası gereği, insanların güvensizliğini azaltmalı, insanları daha fazla güçlendirmeli ve mümkün olduğunca eşitlikçi, saydam ve hesap verebilir olmalı. Dolayısıyla, iyi politika, düzenleme ve hesap verebilirlik önlemlerinin uygulamaya konulması gerekiyor (Roof, 2017, ss. 10-11)."

Değerlendirmeler ve yaklaşımlar hangi yönde ve düzeyde olursa olsun Endüstri 4.0 başlığı altında yapay zeka gibi ileri düzey uygulamalar insanlığı şekillendirmektedir. Her geçen gün kurumlarda, toplumlarda, devletlerde veri işlemede yapay zeka ve robotik sistemler önem kazanmaktadır. Endüstri 4.0, yapay zekâ uygulamaları hayata dair birçok alanda olduğu/olacağı gibi belge yönetimi ve arşiv alanını da köklü değişikliklere uğratacağını söyleyebiliriz. Ancak insanı tümden devreden çıkarmak mümkün olamayacak gibi görünüyor. Yapay zeka teknolojileri arttıkça onları daha iyi besleyen ve daha iyi anlayan insanların değeri de artacaktır.

Gelecek veri bilimcisine ihtiyacın artacağını gösteriyor. Veriye dayalı karar vermeyenlerin ayakta kalamayacakları gerçeğini unutmamak gerekir. Veri bilimcisinin ürettiği veriyi anlayıp, uyarlayacak, işleyecek kişilere ihtiyaç olacak, arşivciler veri bilimci mi olacak, yoksa üretilen veriyi anlayıp, uyarlayacak ve

işleyecek kişiler mi olacak? Analitik bilgi yönetim sistemleri her geçen gün daha fazla önem kazanmaya devam edecek ve bu bağlamda "arşivsel bilgi analizi" (Özdemirci ve Torunlar, 2015) bir değer olarak ortaya çıkacaktır. Arşivciler geleceğin bilgi analistleri olacaktır. Geleceğin belge yöneticileri ve arşivcileri, teknolojiden, siber güvenlikten anlayan, kod yazabilen, yapay zeka ve robotik sistemleri vb. konuları alanına dahil edebilen uzmanlar olmalıdır.

Veri madenciliğinden veri bilimciliğe çıkmak gerekiyor. Veriyi oradan çıkarmak yetmiyor, veriyi anlamlandırmak, veriyi ilk karar verene, en çabuk karar verecek biçime getirip sunmak gerekiyor, temel kavram "veri anlamlandırma" ve bu bir ustalık, bir uzmanlık işidir. Asıl mesele bilginin depolanması değil, yorumlanmasıdır. Belge yöneticisi ve arşivciler sadece belge-bilginin toplanmasında, depolanmasında değil, değerlendirilip analiz edilmesinde etkin olmalıdır. Yapay zeka gibi yenilikçi uygulamaları kullanmalıdır. Bir noktadan sonra kontrol imkânlarımızı sınırlasa da, bazı şeylerin 'elimizin altından kaymakta' olduğunu bize hissettirse de, teknoloji kendi başına bizim kaderimizi belirleme gücüne sahip bir olgu olmamalıdır.

Bilginin işlenmesini hızlandırmak, analiz ve sentez yapmak, karar verme süreçlerini etkilemek ve iş ve işlem ilişkilerinin devamlılığını sağlamak yapay zekânın diğer kullanım alanları arasında ifade ediliyor. Teknolojinin geldiği noktada bireyler veya toplumlar olarak meseleye yalnızca bir mühendislik alanı üzerinden bakmamak gerekiyor. Mühendislik alanından belki daha da etkili ve insanlık tarihini yönlendirecek şey, bilgiyi yapay zekâlara yüklemek olacak. Yapay zekâya kodlar, algoritmalar üzerinden hangi bilgileri yükleyeceğiz, onların bunu geliştirecek yapısallıklarını hangi güzergâha oturtacağız? Yapay zekâlar kodlarını ve algoritmalarını kendileri oluşturmaya başladıklarında gelişim çizgileri hangi yönde olacak? Toplum, kurum kuruluş olarak bizler bu konuda ne kadar hazırlıklıyız, kodlayacağımız, algoritma geliştireceğimiz, yükleyeceğimiz bilgi varlıklarımız ve bilgilerimiz ne kadar düzgün, bilinebilir ve yönetilebilir? Bu sorulara cevaplarımızın hazır olduğunu söyleyebilecek bir noktada değiliz. Bütün bu açıklamalar ışığında şu tespitte bulunabiliriz, yapay zekâ çalışmaları belge yönetimi ve arşiv alanının ayrılmaz parçalarından bir tanesidir ve belge yönetimi ve arşiv disiplini yapay zekanın nimetlerinden sonuna kadar faydalanmalıdır.

Tartışma ve Sonuç

Ankara Üniversitesi bünyesinde yürütülen projede, AI'nin bilgi-belge süreçlerine uygulanabilirliği, kurum hafızasının oluşturulması, geçmiş kararların yeni karar süreçlerine dahil edilebilmesinin yöntemleri araştırılmaktadır. Bu kapsamda, AI algoritmaları tarafından yönetilen iki sanal birim arasında yazışmaların

gerçekleştirilmesi, belli kategorideki belgelerin AI tarafından, geçmiş tecrübelere dayanarak otomatik imzalanmasının zemini, e-dosyalama sisteminin etkin kullanımı, gibi hususlar tartışma ve araştırmanın zeminini oluşturmaktadır.

Belge yöneticisi ve arşivci de, belge ve bilgi birikimiyle ilgili altyapısını iyi kurarak, günümüzün bilgi toplumunun ortaya çıkmasının hem sebebi hem de sonucu olan teknolojiye hâkim olarak, getirdiklerini ve sonuçlarını da analiz ederek, işi tarihin vicdanına havale etmeden hem kendisine hem de kamuya ve topluma dersler çıkartmalı, görünen ve algılanan tüm olumsuzlukları, muhterislikleri evcilleştirip yönetilebilir kılacak süreçleri kurgulayıp gerçekleştirerek mesleki sorumluluk ve inisiyatifini pozitif yönde kullanmalıdır. Bilgi her yerde var, ancak bilgiyi deneyim haline getiren insanların değeri artıyor. Belge yöneticileri ve arşivciler deneyimlerini kullanmayı bilirlerse, geleceğin önemli meslekleri arasında var olmaya devam edecektir.

Kaynakça

A new era: Artificial intelligence is now the biggest tech disrupter. (2017, October 6). *Bloomberg Professional Services*. Retrieved from https://www.bloomberg.com/professional/blog/new-era-artificial-intelligence-now-biggest-tech-disrupter/

AI for Good Global Summit. (n.d.). Retrieved December 12, 2017, from http://www.itu.int:80/en/ITU-T/AI/Pages/201706-default.aspx

Cellan-Jones, R. (2014). Stephen Hawking warns artificial intelligence could end mankind - BBC News. Retrieved December 12, 2017, from http://www.bbc.com/news/technology-30290540

DOWD, M. (2017). Elon Musk's Billion-Dollar Crusade to Stop the A.I. Apocalypse | Vanity Fair. Retrieved December 12, 2017, from https://www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade-to-stop-ai-space-x

Fireman & Co. – A legal industry-focused management consulting firm. (n.d.). Retrieved December 12, 2017, from https://firemanco.com/

Future of Humanity Institute (2017). https://www.fhi.ox.ac.uk/ . Erişim: 12Ekim 2017.

Harari, Y. N., & Genç, E. (2016). *Hayvanlardan Tanrılara sapiens: insan türünün kısa bir tarihi.*

KAUL, A., & WHEELOCK, C. (2016). *Artificial Intelligence Market Forecasts* (Market Research No. 3Q 2016).

Neururer, M. (2015, August 7). Artificial Intelligence in Knowledge Management. Retrieved December 12, 2017, from https://medium.com/artificial-intelligence-ai/the-role-of-artificial-intelligence-in-knowledge-management-309973209cfd

Özdemirci, F. "Belge ve Arşiv Yönetiminde Yeni Ufuklar ve Kuramsal Yaklaşımlar". **Bilgi ve Belge Yönetimi: Kuramsal Yaklaşımlar**/ Yayına hazırlayanlar: Bülent Yılmaz, Turgay Baş, Semanur Öztemiz, Meltem Dişli.- İstanbul: Hiperlink, 2017. İçinde 219-232. ss.

Özdemirci, F., Torunlar, M.(2015). Bilgi Çağında Arşivsel Bilgi Analizi: Bilgi-İktidar-İdeolojo-Devlet. Ankara.

ROOF, Heather M. (2017, Temmuz). Teknoloji, Değerler ve İnsan Güvenliği Yapay Zekâ Yoluyla İnsan Güvenliğinin İlerletilmesi. Turquie Diplomatique, sayı: 99, İstanbul.

Solon, O. (2017, September 28). Deus ex machina: former Google engineer is developing an AI god. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2017/sep/28/artificial-intelligence-god-anthony-levandowski

Will Robots Take My Job? (2017) https://willrobotstakemyjob.com/ . Erişim: 12 Ekim 2017.

Wyatt, P., & Ryan, E. (2017, June 25). How artificial intelligence is streamlining document management. Retrieved December 12, 2017, from https://www.lawyersweekly.com.au/biglaw/21348-how-artificial-intelligence-is-streamlining-document-management

Elektronik Belge Yönetimi, Dijital Arşivleme Sistemleri ve Büyük Veri

Uzm. Korcan DOĞAN

Ankara Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Prof. Dr. Sacit ARSLANTEKİN

Ankara Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Özet

Bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle birlikte büyük veri kavramı ortaya çıkmıştır. Bu kavram yeni bir devrin başlangıcı olarak yorumlanmaktadır. Arşivlerin ve elektronik belge yönetim merkezlerinin de bu gelişmelerin dışında kalmaları mümkün değildir.Bu merkezlerde ve kullanılan uygulamalarda yalnızca yapılandırılmış verilere değil, yapılandırılmamış verilere olan ihtiyaç da giderek artmaktadır. Özellikle veri ve metin madenciliği gibi analitik vb. işlemler için büyük veri teknolojilerinin kullanılması ise bu sistemlerdeki özellikle yapılandırılmamış veriler aracılığıyla büyük fırsatlar sunmaktadır. Elektronik belge yönetim sistemleri ve dijital arşivlerdeki veri, yapılandırılmamış verilerin de eklenmesiyle büyük veriyi niteleyen unsurlarda olduğu gibi hacim, hız ve çeşitlilik yönünden hızla büyümektedir. Bu büyük veri yığını içinde yapılandırılmış verilerden enformasyon üretmek üzere sorgulama ve erişim yapılabilirken, yapılandırılmamış ve bir çeşit örtük veri niteliğindeki verilerden istenilen nitelikte sorgulama yapılamamakta; kurumların yararına kullanılacak enformasyon üretilememektedir. Veri madenciliği, metin analitiği vb. analitik yöntemler kullanılarak, veri ambarlarında toplanacak bu örtük veriler de işlenebilir nitelik kazanmaktadır. Bu teknikler ile veri yığınları işlenerek, kurumların karar destek sistemleri için gerekli enformasyon ve öngörüler üretilebilmektedir. Çalışma kapsamında "büyük veri" ile Elektronik Belge Yönetimi ve Dijital Arşivleme Sistemleri arasındaki ilişki, bu sistemlerin ne gibi veriler depoladığı, daha ne tür veriler toplayarak bu sistemler için katma değer sağlayabileceği konuları ele alınacaktır.

Anahtar sözcükler: *Büyük Veri, EBYS, DYS, Elektronik Belge Yönetim Sistemleri, Dijital Arşivleme Sistemleri, Veri Madenciliği.*

Giriş

Gelişen bilgi ve iletişim teknolojilerinin kapsamında kabul edilen internet teknolojileri; web sayfaları, bloglar, sosyal medya uygulamaları, sensörler ve

daha pek çok veri toplayan cihaz ve uygulamalar sayesinde her an, her türlü veri toplanabilir hale gelmiştir. Bu veri yığının değerinin anlaşılması sonucunda, bu veriyi toplama, işleme, kullanıcılara hazır hale getirme, erişime sunma, saklama, analiz etme gibi aşamalarda pek çok farklı teknikler de kullanılabilmektedir (Doğan & Arslantekin, 2016, s. 15). Toplanan bu veriler, pazarlama, halkla ilişkiler, bankacılık, güvenlik vb. pek çok alanın yanında elektronik belge yönetim sistemleri ve dijital arşivlerde de kullanılabilir nitelik taşıyabilmekte; bu verilerin işlenmesiyle kullanıcılarının gereksinimlerini daha iyi anlayarak memnuniyeti arttırmakta ve hizmetlerini geliştirebilmektedirler.

Bu verilerin günümüzde hız, çeşitlilik, kapasite (hacim) açısından büyük artış göstermesi ve bu artışa teknolojinin de destek vererek, yeni çözümler üretmesi ile birlikte "Büyük Veri" kavramı ortaya çıkmıştır. Yaşanan gelişmelerle birlikte büyük veri kavramına hazırlıksız yakalanan kurum/kuruluşlar ve bireyler için bu durum; gerek ilgili sistemlerinde bulundurmaları bakımından, gerekse işlem ve hizmetlerinde kullanmaları bakımından son derece önemli hale gelmiştir. Bu veriyi kullanabilenler, diğerlerine göre avantajlı hale gelmekte, iş yapılarını geliştirmekte, ar-ge ve uygulama faaliyetlerini daha rasyonel gerçekleştirebilmektedir. Konuyla ilgili oluşturulan yeni teknikler sayesinde atıl durumda bulunan verilerin ilişkilendirilerek katma değer yaratan enformasyon haline getirilebilmesi sağlanabilmiştir (Doğan & Arslantekin, 2016, s. 15,16).

Çalışmamızda öncelikle büyük veri ve ilgili kavramlar değerlendirilecektir. Devamında dünyada elektronik belge yönetim sistemleri ve arşivlerle ilgili uygulamalar verilecek ve bu alanla ilgili yapılabilecek ve yapılması gereken çalışmalara yer verilecektir.

Büyük Veri

Verinin, günümüzde organizasyonlar için çok büyük avantajlar ve fırsatlar sunmaktadır. 2012 yılında Davos'taki Dünya Ekonomik Forumu'nda tıpkı para, altın gibi varlıklara ek olarak, yeni bir ekonomik değer olarak "veri" den bahsedilmiştir. Bir değer olarak kabul edilmesine karşın, verinin ekonomik değerini bulmak oldukça zordur. Bir başka deyişle verinin kişi, kurum kuruluş vb.lerine ekonomik katkısını rakamlarla ifade edebilmek oldukça güçtür. 2011 yılında Amerika Birleşik Devletleri'nde 17 endüstri sektöründen 15'indeki şirket başına düşen veri miktarı, Birleşik Devletler Kongre Kütüphanesinin sakladığı 235 Terabayt veriden daha çoktur. Wal-Mart Mağazaları Şirketi her saat bir milyondan fazla müşterinin veri işlemini veri tabanında saklamak zorunda kalmaktadır ve sakladığı veri miktarı 2,5 petabayta ulaşmıştır. Bu rakam Kongre Kütüphanesinin elinde bulundurduğu veri miktarının yaklaşık olarak 167 katıdır. Yine bunlara benzer olarak 2010 yılında 5 milyar cep telefonu kullanılmıştır ve 30 milyar adet Facebook içeriği paylaşılmıştır (Johnson, 2012, s. 51-52).

Günümüzde pek çok kuruma yalnızca kendilerine ait operasyonel veri tabanları yetmemektedir. Dış kaynaklardan alınan verilerle çeşitli analizler yapılarak yeni bilgilerin üretilmesi ve bu bilgilerin kurum içi süreçlerde kullanılması ihtiyacı doğmuştur. Yaygın olan ve alışılmış veri tabanı yönetim sistemleri ise dış kaynaklardan gelen bu verilerin kurum içi enformasyonun yönetiminde kullanılması konusunda yeterli desteği verememektedirler. Çünkü dış kaynaklardan alınan veriler hem kendi operasyonel veri tabanlarına kolaylıkla aktarılabilir nitelikte hem de yapılandırılmış durumda olmayabilmektedir. Bu nedenle günümüzde pek çok büyük bilişim ve teknoloji şirketi büyük veri konusunda çok büyük miktarlarda yatırımlar yapmaktadır (Doğan & Arslantekin, 2016, s.21).

Francis X. Diebold, büyük veri kavramının ilk defa Silicon Graphics (SGI)'den John Mashey[1] tarafından 1998'de *Büyük Veri ve Altyapı Gerilimi Dalgası* (Big Data and the Next Wave of InfraStress) isimli sunumunda kullanıldığını belirtmektedir (Diebold, 2012, s. 3). Halen Gartner'ın bir parçası olan Meta Group isimli şirket ise, 2001 yılında büyük veriyi niteleyen hacim, hız ve çeşitlilik konularından bahsetmiştir (Laney, 2001). Günümüzde her ortamda büyük veri, 3V ile anılmaktadır. Büyük verinin bu terimler ile nitelendirilmesi Meta Group'un literatüre önemli bir katkısıdır (Doğan & Arslantekin, 2016, s22).

Büyük veri genel olarak kullanılan programların saklama, yönetme ve işleme kapasitesinin ötesindeki veri kümelerini anlatmak için kullanılan bir terimdir. Büyük verinin devasa boyutları ile bundan fayda sağlamak için gereken analizlerin karmaşıklığının birleşmesi, yeni sınıf teknolojilerin ve bunları yönetecek araçların gelişmesine neden olmuştur. Aslında büyük veri genelde hem yönetilen verinin türünü, hem de onu depolamak ve işlemek için kullanılan teknolojiyi anlatmaktadır. Bu teknolojilerin büyük bir kısmı Google, Amazon, Facebook ve LinkedIn vb. şirketlerin inanılmaz büyük sosyal medya verisi ile uğraşırlarken kendileri için geliştirdikleri teknolojiden doğmuştur. Bu şirketler doğası gereği, düşük maliyetli hazırda bulunan donanım ve açık kaynaklı yazılımlara önem vermektedirler (Cackett, 2013, s. 14).

Büyük veri genellikle birbirlerinden farklı veri kaynaklarından toplanan geniş veri dermelerinin analizi, işlenmesi ve depolanması ile ilgili bir alan olup; çözümlerinin ve uygulamalarımın karakteristik, yani kendine özgü olması gerekmektedir. Geleneksel veri analizi işlemleri, depolama teknolojileri ve teknikleri yetersiz kalmaktadır. Spesifik olarak büyük veri, çoklu ilişkisiz veri kümelerinin birleştirilmesi, büyük miktarda yapısal olmayan verinin işlenmesi,

---

[1] Mashey'in bu sunumuna https://www.usenix.org/legacy/event/usenix99/invited_talks/mashey.pdf adresinden ulaşılabilir.

gizli enformasyonun kısıtlı zaman içinde toplanması gibi farklı gereksinimlere işaret etmektir (Erl, Khattak, & Buhler, 2016, s. 19).

McKinsey Global Institute, 2011 yılında büyük veri kavramını, tipik ve geleneksel veri tabanı yazılımlarının yapamayacağı şekilde, bunların kabiliyetlerinin ötesinde, veri kümelerini alan, saklayan, yöneten, erişime sunan ve analiz eden araçları tanımlamak için kullanmıştır (Manyika, ve diğerleri, Mayıs 2011, s. 1). Bu tanım, konusu büyük veri olan Kord Davis ve Doug Patterson'ın, *Ethics of Big Data* (Davis & Patterson, 2012, s. 4) gibi başka yayınlarda da kullanılmış olduğundan konu açısından önem taşımaktadır.

Ancak unutmamak gerekir ki büyük verinin yalnızca verinin hacmi nedeniyle büyük olduğu söylenemez. Büyük verideki "büyük" kelimesi verinin işlenme sürecindeki önemini ve etkisini de kapsamaktadır. Açık veri ile bu miktar devamlı olarak artmıştır (Monino & Sedkaoui, 2016, s. XXXIV).

Büyük Veriyi Niteleyen Unsurlar

Görüldüğü üzere büyük veri tanımları çok büyük kesinlik taşımamaktadır. Belki büyük veri zamanla değişecek ve bugünün büyük verisi gelecekte aynı anlama gelmeyebilecektir. Bu yüzden büyük veri kavramının tanımlamasında yardımcı olması için genellikle verinin hacmi, hızı ve çeşitliliğini ifade eden "3 V" (volume, velocity, variety) notasyonu, yaygın olarak onu diğer veri türlerinden ayıran kavramlar olarak kullanılmaktadır. Nitekim büyük veri kavramının tanımlanmasındaki değişim günümüzde bile kendini göstermektedir. Literatürde 3V'ye "verinin değerini" (value) ekleyerek 4V ile tanımlayanlar da bulunmaktadır (Cackett, 2013, s. 14).

Verinin hacmi, verinin büyüklüğü ve boyutunu ifade etmektedir. Verinin boyutunu rakamsal bir şekilde belirtmek genelde çok kısıtlayıcı olmaktadır. Çünkü teknoloji ilerledikçe, rakamlar hızlı bir şekilde değişmektedir ve kısıtlayıcı rakamlar artık geçerliliğini yitirmektedir. Bu yüzden verinin göreceli miktarını belirtmek daha faydalı olmaktadır. Eğer ilgilenilen verinin miktarı daha önce kullanılan verinin üstündeyse muhtemelen büyük veri ile uğraşılmaktadır. Bu bazı kurum/kuruluşlar için onlarca terabayt olurken, bazıları için onlarca petabayt olabilmektedir (Cackett, 2013, s. 14).

Günümüzde artık pek çok cihaz veri üretebilir hale gelmiştir. Gerek bireylerin ve kurumların sakladığı verilerin, gerekse de internet dünyasında saklanan verinin büyüklüğü zaman geçtikçe artmaktadır. Veri depolama birimlerinin fiyatlarındaki hızlı düşüş, saklanan verilerin oranının geometrik şekilde hızlanarak artmasında önemli bir etken olmaktadır. Eskiden yalnızca operasyonel veri tabanlarının kullanılması yeterli olurken şimdi ise, bilgi ve iletişim teknolojilerinde yaşanan gelişmeler doğrultusunda, veri ambarlarında toplanan bütün veri işlenip analiz edilebilir hale gelmiştir (Doğan & Arslantekin, 2016, s. 24).

Verinin hızı, elde edilen veri ile ilgili gerçek zamanlı (anlık) olarak harekete geçilebilmesini ifade etmektedir. Her ne kadar gerçek veri analizinin verinin geldiği dönemle aynı anda tamamlanması mümkün olmasa da; uygulamaya geçmedeki gecikmeler kaçınılmaz olarak yapılması istenen ve beklenen çalışmaların verimliliğini kısıtlamakta, müdahale etmeyi zorlaştırmakta ve optimal olmayan süreçlere yol açmaktadır. Örneğin coğrafi konum olarak müşterinin nerede olduğuna dayanarak yapılan bir indirim/promosyon teklifi; müşteri o noktadan geçtikten sonra müşteriye ulaşırsa, başarılı olma şansı çok düşebilecektir (Cackett, 2013, s. 14).

Günümüzde bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, verinin üretildiği anda kullanılmasına olanak vermektedir. Hızla akan veriye en hızlı tepkinin verilerek, daha veri akarken müdahale etmek, işlemek ve analiz etmek olanaklı hale getirmiştir. Verinin bu hızına yetişebilen firmalar daha veri üretildiği anda yanlış yapılan bir işleme müdahale edebilmekte; bu veriler ortaya çıktığı anda kurumlar kendi analiz süreçlerine katabilmekte; karar destek sistemlerindeki analiz süreçlerine aynı anda bu veriler eklenip kullanılabilmektedir (Doğan & Arslantekin, 2016, s.24).

Verinin çeşitliliğinin söz dizimi (syntax) ve semantik (anlamsal) olmak üzere 2 boyutu vardır. Geçmiş dönemlerde bu iki boyut, hangi verinin güvenilir bir biçimde veri tabanlarında yapılandırıldığının ve analizin içeriği için ne kadar güvenilir olduğunun derecesini belirlemekteydi. Modern ETL[2] araçları görsel olarak gelen sanal sözdizimi verilerini çok başarılı bir şekilde işleyebilirken, serbest metin gibi semantik olarak zengin verilerin çözümünde daha başarısızlardır. Bu yüzden birçok organizasyon, enformasyon yönetim sisteminin veri kapsamını daha dar bir veri düzeni ile sınırlamışlardır. Bu sınırlamayı organizasyonların daha kapsayıcı, ek değer yaratması takip etmiştir ve bu muhtemelen Büyük Veri yaklaşımının en çekici olan özeliklerinden biridir (Cackett, 2013, s. 15).

Günümüzde veri, geçmişte olduğu gibi sadece yapılandırılmış veriden değil, aynı zamanda yapılandırılmamış verilerden de oluşmaktadır. Bu veriler bilinen ve yeni kabul edilen ortamların yanında gittikçe artar duruma gelmiştir. Hatta bazı büyük web siteleri kullanıcılarının imlecini nerelerde gezdirdiğinin ve web kullanım bilgilerini bile veri olarak saklamaktadırlar. Bu çeşitlilik hem kendi arasında, hem de alt dallarıyla birlikte her geçen gün hızla büyümektedir. Büyük veri ile birlikte günümüzde tüm bu veriler iş süreçlerinde de kullanılabilir hale gelmiştir (Doğan & Arslantekin, 2016, s.25).

---

[2] ETL: Extraction,transforming ve load işlemlerinin kısaltması . Şirketlerin networklerinde farklı yerlerde / veri tabanlarında olan bilgilerin oradan alınması (extraction), temizlenip belli bir formata dönüştürülmesi (transforming) ve veri madenciliği yapılacak veri tabanına yüklenmesini (load) belirtir.

Çalışmanın başlarında büyük verinin oluşumunda pek çok farklı kaynaktan veri toplandığından bahsedilmişti. Bu doğrultuda günümüzde veri sağlayan pek çok araçtan söz edilebilir. Bu bağlamda da karşımıza bir başka yeni kavram olan "Nesnelerin İnterneti" çıkmaktadır (Doğan & Arslantekin, 2016, s.25).

Nesnelerin İnterneti

Nesnelerin interneti, her gün kullanılan nesnelerin içine çipler, sensörler ve iletişim modülleri yerleştirilerek, kısmen çevrimiçi ağ oluşturmakla, ama bundan da daha çok insanları çevreleyen her şeyi verileştirmekle ilgili bir kavramdır. Dünya bir kere verileştirildiğinde, bilginin potansiyel kullanımları temel olarak sadece kişinin marifetleri ile sınırlı olabilecektir. Verileştirme, insanın kavrayışında temel bir zenginleşmeyi temsil etmektedir. Büyük veri ile birlikte, bundan böyle dünya temel olarak bilgiden oluşan bir evren olarak görülebilecektir (Schönberger & Cukier, 2013, s. 103-104).

Birbirlerine bağlanan ve birbirleriyle haberleşen cihazların artması, nesnelerin interneti ile birlikte veri patlamasına neden olmakta, veri patlaması sonucu büyük veri oluşmakta ve bununla birlikte günümüzde verinin analiz edilmesi ile ilgilide önemli sorunlar doğurmaktadır. Büyük veriyi depolamak ve erişime sunmak kadar, analizi içinde yeni yaklaşımlar ve yöntemler geliştirilmektedir. Bu yöntemlerin en başında veri madenciliği ve metin madenciliği gelmektedir (Doğan & Arslantekin, 2016, s. 26).

Veri Madenciliği

Veri madenciliği, elde edilen büyük verinin analiz edilmesinde kullanılabilecek en önemli yöntemlerden biridir (Doğan & Arslantekin, 2016, s.26).

Veri madenciliği, veriden bilgi keşfi olarak da tanımlanabilir. Veri madenciliğinde otomatik ve kısmi otomatik metotlar kullanılarak büyük miktarlı veriden bilgi çıkarımı hedeflenir. Veri madenciliği veriden modeller geliştirmek, ilgi çekici yapılar veya yinelenen temalar bulmak vb. için istatistik, yapay zeka, bilgisayar bilimi gibi çeşitli bilim dallarından algoritmalar kullanmaktadır. Veri içindeki kullanışlı enformasyonun ve mümkün, anlamlı ve kullanışlı ilişkilerin bulunabilmesi için veritabanı enformasyonunu analiz edebilen bütün teknolojileri bir araya getirmektedir (Monino & Sedkaoui, 2016, s. XIII).

Arslantekin (372-373), veri madenciliğini *"büyük miktarda veriden anlamlı bilgi çıkarma sanatıdır. Toplanan büyük yığın halindeki veriler arasında örnek kalıpların tanımlanması, eğilimlerin belirlenmesi ve gerekli ilişkilerin kurulması işlemlerine ait bir süreçtir"* şeklinde belirtmiştir.

Veri madenciliği birçok disiplinin katkıları ile inşa edilmiş bir yapıdır. Bu yapının taşıyıcı birimleri ise yapay zeka, veri tabanı yönetim sistemleri ve çok değişkenli istatistik analiz teknikleridir. Son yıllarda ise bu disiplinlere yeni disiplinler

katılmaktadır (Akpınar, 2014, s. xiii). Veri madenciliği bu bağlamda büyük veri ile yapılan yapay zeka çalışmaları için de son derece önemlidir.

Veri madenciliğini büyük veri bağlamında değerlendirecek olursak, elde edilen büyük verinin içinde gizli olan enformasyonun önceden güvenilirliği kanıtlanmış istatistiksel tekniklerle ortaya çıkarılmasıdır şeklinde tanımlayabiliriz. Büyük verinin analizinde en temel yöntemlerden birisi olması nedeniyle veri madenciliği bu konuda son derece önemlidir (Doğan & Arslantekin, 2016, s.27).

Metin Madenciliği

Özellikle web ortamından elde edilen metin halindeki büyük verinin analiz edilmesinde metin madenciliği önemli bir istatistiksel tekniktir. Kimi zaman metin halindeki veriler sosyal medyadan elde edildiğinde buna sosyal medya madenciliği, web üzerinden elde edildiğinde buna web madenciliği gibi tanımlar yapılsa da ve her birinin kendine özgü yöntemleri olsa da, bunların geneli temel olarak veri madenciliği ve metin madenciliğine dayanmaktadır (Doğan & Arslantekin, 2016, s.27).

Metin madenciliği geniş hacimdeki metin içeriklerinin ana eğilimlerini çıkarmak ve farklı konulardaki uğraşıları istatiksel değerlemek için süreçleri otomatikleştirmeyi mümkün kılan bir tekniktir (Monino & Sedkaoui, 2016, s. XVI).

Metin madenciliğini oluşturan temel alanlar istatistik, veri madenciliği, doğal dil işleme, web madenciliği ve bilgi erişimidir (Oğuzlar, 2011, s. 20).

Doğal dil metinlerindeki örüntülerle ilgilenen ve yeni, eski veya bilinmeyen enformasyonu keşfetmek amacıyla doğal dil işleme, veri madenciliği ve bilgi erişim tekniklerinin uygulayan teknolojidir. Metin madenciliği birbirleriyle ilişkili metinlerden oluşan kaynakları bir araya getirmek için, bunları analiz etmek ve tanımlamak için, anahtar varlıkları ve bunların özelliklerini içeren nitelikleri çıkarmak için ve çıkarılmış nitelikleri birleştirmek için, yeni nitelikleri şekillendirmek için veya değerli içgörü kazanmak için kullanılabilir (Prytherch, 2005, s. 688).

Yukarıdaki tanımlarda göstermektedir ki her tanım farklı farklı noktalara değinebilmektedir. Metin madenciliği, "pek çok farklı ortamdan olabileceği gibi özellikle web ortamından elde edilen yapısal olmayan metin türündeki verilerin içindeki gizli enformasyonun çıkarılmasını sağlayan, bu enformasyonun çıkarılması sırasında metinlerin içindeki ilişkileri bulan ve bunları çeşitli kalıplarda ifade edilmesine olanak sağlayan, bu kalıplara dayanarak geleceğe yönelik tahminlerde bulunulmasına olanak veren istatiksel analiz yöntemidir" şeklinde de tanımlanabilir (Doğan & Arslantekin, 2016, s.28).

Dünyada Büyük Veri ve Arşiv Uygulamaları

Elektronik belge yönetimi ve dijital arşiv sistemlerinde büyük veri kullanımını daha iyi kavrayabilmek ve geliştirebilmek için dünyada büyük veri konusunda çalışma yapan ve konuyla ilgili stratejilerinde büyük veriye yer veren bazı milli arşivlere yer vermekte fayda bulunmaktadır.

E-Ark Projesi, Danimarka, Norveç, Estonya, Slovenya, Portekiz ve Macaristan Pilot Uygulaması:

E-ark Projesi çeşitli Avrupa Birliği ülkelerinin katılımıyla gerçekleşen ve Danimarka, Norveç, Estonya, Slovenya, Portekiz ve Macaristan da pilot olarak uygulanan, Avrupa çapında arşiv çalışmalarını tutarlı bir hale getirmek için dijital arşivleme yöntem ve teknolojilerini geliştirmeyi amaçlayan çok uluslu bir büyük veri projesidir (E-ARK Project, 2017).

E-ARK projesi, bağımsız belge saklama teknolojileri, sistemleri ve uygulamaları ile ilgili bir takım sorunları çözerek,

- uluslararası arşivlerin geliştirilmesi,
- teknik şartnamelerin ve araçların sağlanması,
- entegre bir arşivleme altyapısının geliştirilmesi,
- erişilebilirliğin, erişimin ve kullanımın geliştirilmesi ve
- toplu arşiv verilerinin detaylı analizi gibi konuları kapsamaktadır (E-ARK Project, 2017).

Proje 2014 ile 2017 yılları arasında, Avrupa Komisyonu tarafından BİT Politika Destek Programı (PSP), Rekabet Edebilirlik ve Yenilikçilik Çerçeve Programı (CIP) kapsamında ortaklaşa finanse edilmiştir.

Projede veri depolama ve analizi için açık kaynak kodlu Cloudera CDH4 dağıtımının Apache Hadoop üstünde bir veri yönetimi ve depolama katmanı benimsenmiştir (E-ARK Project, 2017).

E-ark projesi aşağıdakileri sağlamıştır:

- açık arşiv ürünleri (araçlar, hizmetler, meta veri özellikleri),
- açık teknik ürünler, açık operasyonel ürünleri (erişim araçları, hizmetleri, meta veri spesifikasyonları),
- iş zekası için veri madenciliği araçları da dahil olmak üzere açık erişim araçları, hizmetleri vb. (E-ARK Project, 2017).

A.B.D Milli Arşivleri 2014-2018 Yılları Arası Stratejik Planı

2014- 2018 yılları arasını kapsayan stratejik planda elektronik belgelerin A.B.D Milli Arşivleri (NARA - The U.S. National **Archives** and Records Administration) için büyük zorluklar ve fırsatlar yarattığı vurgulanmıştır. Bu strateji kapsamında Elektronik belgelerin yönetimini, korumasını ve erişimini

geliştirmek için çalışmaların yer aldığından bahsedilmiştir (U.S. National Archives and Records Administration, 2014).

A.B.D. Milli Arşivleri, giderek daha büyük hacimli elektronik kayıtları, daha büyük dosya boyutlarında ve çeşitli biçimlerde yönetmek için kayıtların kabul, saklama ve kamuya açık erişim yaklaşımını modernleştirmek amacındadır. Stratejik planda, Büyük verinin sosyal medya ve kamuya açık veriler ile hükümet verilerini yeniden kullanma becerisini, özellikle devlet kayıtlarının geleneksel kayıt yönetimi uygulamalarına alternatif olarak önemli ölçüde değiştirdiği vurgulanmıştır (U.S. National Archives and Records Administration, 2014).

Birleşik Krallık Milli Arşivleri, 2017 Stratejik Planı:

Birleşik Krallık Milli Arşivleri, 2017 dijital stratejisinde, bütün dünya arşivlerinde olduğu gibi önlerindeki dijital zorlukları şu şekilde açıklamıştır:

- Belgeler fiziksel ortamdan sanal ortama taşınmaktadır: Dijital kayıtlar, fiziksel belgelerden çok farklıdır. Kayıtlar yalnızca belgelerden değil, web tabanlı bir araç, video, web sitesi, yapılandırılmış veri kümeleri ve bilgisayar kodları vb. her türlü içerikten oluşabilmektedir. Dijital kayıtlar, genellikle, farklı içerik oluşturucuların ve sahiplerinin potansiyel olarak farklı bileşenlerden oluşan bir bileşimidir. Büyük dijital kayıt koleksiyonlarını nispeten kolayca hesaplanabilir, neyin önemli olabileceğini anlamak ve potansiyel olarak önemli öğeleri bulma maksadıyla arama yapmak için veriler kullanılabilir. Bu yaklaşım neyin değerli olabileceğini değiştirebilir ve değerlendirme-seçim yaklaşımlarını etkileyebilir. Kayıtların içeriği de farklı şekillerde tanımlanabilir. Bağlamsal veriler daha akıcı ve birbirine bağlı hale gelebilir.
- Dijital koruma zordur: Dijitalleşme ile birlikte arşivlerde koruma için uzun vadeli bir çözüm bulunmamaktadır. Kayıtların mevcut olmaya devam edebilmesi için tüm arşivlerin yapması gereken şey, mühendislik çabasıyla, teknolojik değişim devam ettikçe ve nesiller boyunca, yatırım yapmaya devam etmek için kurumsal taahhüdü sağlamaktır. Bu taahhüt birkaç şeyi içermektedir. Birincisi, dijital kayıtlar için geçerli uzun vadeli veri depolama ortamı olmadığı için bitleri korumaktır; zamanla, kopyalar yapılmalı ve her kopya aynı olmalıdır. İkincisi, kaydın üretimini veya kullanılmasını sağlamaktır. Dijital kayıtlar, koda bağlı olan verilerdir. Bu veriler kendiliğinden olabilir veya kod içerebilir. Dijital arşiv, karmaşık bir bağımlılık kümesini anlamalı ve yönetmelidir: kod hakkındaki veriler, diğer koddaki kod, veri üzerinde kod. Ayrıca, bu bağımlılıkları zamanla ve teknolojik değişim nesilleriyle yönetmek gerekmektedir. Bir arşiv, neyin korunacağını bildiği zaman, arşivin uzun vadeli koruma risklerini yönetmesi daha kolay hale gelir.
- Beklentiler değişmektedir: Kullanıcıların dijital ürünlerden beklentileri yüksektir. İşlemlerin basit olması, sonuçların derhal olması için servislerin sezgisel olmasını beklemektedirler. Artan beklentilere ayak uyduran servislerin yanı sıra insanların bilgiye nasıl erişip bunları nasıl tükettiklerinde değişiklikler yapmamız gerekmektedir. Mobil cihazlara ve tabletlere kayma gibi eğilimler önemli bir etkiye sahiptir. Arşivler erişim ve kullanımla ilgili değişen beklentilere cevap vermek zorundadırlar. Dijital kayıtlar sunum biçiminde değildir. Dijital bir kayıt oluşturmak için, arşivin, son kullanıcının teknik özelliklerini dikkate alarak, korunmakta olan verilerin nasıl işleneceğine karar vermesi gerekir. Dijital kayıtların (belge biçimleri, e-posta, multimedya, veri kümeleri, kod) çeşitliliği ve değişen kullanıcı ortamları (Masaüstü PC'lerinden tabletlere ve akıllı telefonlara) bunu güçleştirmektedir.
- Değişim sürekli hale gelmiştir: Kayıtların doğası değişmektedir. Bilgisayar kullanımı bize bilgi kaydetmek ve iletişim kurmak için yeni yollar sunmaktadır. Bilgisayarlar ilk kez kamu kurumlarında kullanılmaya başladığında, kağıt üzerinde manuel olarak gerçekleştirilen

çalışma yöntemleri genellikle dijital olarak simüle edilmiştir. Dijital dönüşüm projeleri, hükümetin eski kağıt işlemlerinin dijital simülasyonundan geçmesini sağlamaktadır. Google Dokümanlara veya tweet'e eşdeğer bir kağıt ise bulunmamaktadır. Her yeni teknoloji, dijital arşiv için yeni bir zorluklar getirmektedir ve bu değişim süreklidir. On yıl önce büyük veri analizi, dağıtılmış bilgisayar teknolojisi veya nesnelerin internetinden endişe edilmezken günümüzde gelinen nokta ortadadır. Dijital arşivler, sürekli gelişen teknolojik değişime ayak uydurabilmelidir.

- Arşivlerin kapasitelerine ve yeteneklerine göre, özellikle dijital yeteneklere yatırım yapması gerekmektedir: Özellikle, 'dijital üreticiler', yeni teknolojileri icat edebilen ve uygulayabilen, işgücü piyasasında en çok talep gören kişilerdir. Bunlar, dijital arşivlerin tüm diğer zorluklarla mücadele etmeleri gereken becerileri tam anlamıyla taşıyan özelliklerdir. Arşivler, işgücü piyasasında, ihtiyaç duydukları dijital becerileri olan kişileri işe almak için daha fazla rekabet etmektedir ve bu kişileri daha zor bulmaktadır (The National Archives, 2017, s. 3-5).

Birleşik Krallık Milli Arşivleri 2017 dijital strateji raporunda, on yıl önce büyük veri analizi, dağıtılmış bilgisayar teknolojisi veya nesnelerin interneti gibi konulardan endişe etmediklerini belirtmiştir (The National Archives, 2017, s. 4). Günümüzde ise dijital kayıtların doğru yollarla (büyük veri, yapay zeka ve benzeri tekniklerle) işlenmesiyle yaratacağı katma değerin önemi vurgulanmıştır (The National Archives, 2017, s. 10). Stratejik plan için hazırlanan bu raporda aynı zamanda, Devlet arşivlerinin çalışmamızda da yer verilen **"Hukuk için Büyük Veri"** ve **"Zamanda İzler"** projelerinde elde ettiği büyük veri deneyimlerine dayanarak, bundan sonra yapılacak dijital araştırma projelerine öncülük etme ve/veya işbirliği yapma fırsatı sunulabileceği belirtilmiştir (The National Archives, 2017, s. 13).

Birleşik Krallık ve A.B.D. Milli Arşivlerinin stratejik planlarında, dijitalleşme ve beraberinde yaşanan dönüşüm ile birlikte karşımıza çıkabilecek zorluklar ile dönüşümün yaratacağı fırsatlar karşısında büyük veri konusuna verdiği önem, konu bağlamında son derece önemlidir.

Hukuk için Büyük Veri Projesi

Bu projenin amacı, "research.legislation.gov.uk" adresinde yeni bir Hukuk Kaynakları Veri Araştırma Altyapısını büyük veri araştırmasıyla gerçekleştirmektir (HM Government, 2015).

Araştırma için üç temel alan aşağıdaki gibidir:

1) Araştırmacıların ihtiyaçlarını anlamak,

2) Örtük veriden yeni açık veriler elde etmek.

3) Hukuk kaynakları için uyumlu model dili (pattern language) oluşturmaktır (HM Government, 2015).

Zamanda İzler Projesi

Birleşik Krallık Devlet Arşivleri "Zamanda İzler" projesi ile büyük veri kullanımını tarihi araştırmalarda ilişkili sonuçların getirilmesi çerçevesinde ele almaktadır. Proje kapsamında ilk aşamada Birinci Dünya Savaşı Fonu içerisindeki ilişkili kayıtlar büyük veri analizi ile belirlenmiş, ikinci aşamada ise kullanıcıların erişimi düşünülerek belirlenen ilişkilendirmeler tarama sonuçlarına yansıtılmıştır (The National Archives, 2016).

Araştırmacıların daha fazla sonuca erişebilmeleri için büyük veri teknolojileri ile değerlendirilerek, yapılan arama ile ilişkili sonuçlar getirilerek, tarihte gizli kalmış kişilerin ve öykülerinin kullanıcılarla buluşması sağlanmaktadır (The National Archives, 2016).

Projenin sonunda tarihçiler, soybilimciler gibi farklı disiplinlerdeki araştırmacıların büyük veri araç ve kaynakları kullanılarak ilişkili verilere ulaşması hedeflenmektedir (The National Archives, 2016).

Malezya Devlet Arşivleri Tarafından "Elektronik Belge Yönetimi Ve Arşivlerin Yönetimi Politikası" Kapsamında Oluşturulan "Elektronik Belgelerin Yapısal Olmayan Çevrede Yönetilmesi" Konulu Rehber

Bu rehberin amacı yapısal olmayan elektronik belgelerin yönetiminde kılavuzluk etmektir (National Archive of Malaysia, s. 1).

Malezya Devlet Arşivleri içinde herhangi bir iş akışı olmadan belge ve diğer kayıtların yaratıldığı durumlarda (fiziksel formundan bağımsız olarak), bu yapısal olmayan verilerin kontrol altına alınabilmesi kayıt tutma açısından önemli sorun olarak görülmektedir. İlgili arşiv düzenli çevrenin aksine, düzensiz çevrede de elektronik belgelerin tüm yaşam döngüsü yönetilmesi gerektiğini vurgulamaktadır (National Archive of Malaysia, s. 1).

Bu rehber daha çok e-posta ve benzeri kayıtlar üzerinde yoğunlaşmaktadır.

"Elektronik Belgelerin Yapısal Olmayan Çevrede Yönetilmesi" isimli rehber yapısal olmayan dijital evrendeki kayıtların kontrol altına alınması bakımından son derece önemlidir.

Elektronik Belge Yönetimi, Dijital Arşivleme Sistemleri ve Büyük Veri

Günümüzde arşivlerde yalnızca yazılı veya anlaşılabilir içerikler değil aynı zamanda soyut olmayan bitlerden, veriden ve koddan oluşan dijital kayıtlar bulunmaktadır. Dijital kayıtların zorluğu yüzünden arşivlerin bazı büyük değişiklikler yapması gerekmektedir. Dijital arşivlerle birlikte arşivlerde yeni bir dönüşüme girildiği gerçeği ise yadsınamaz bir şekilde karşımıza çıkmaktadır (The National Archives, 2017, s. 2).

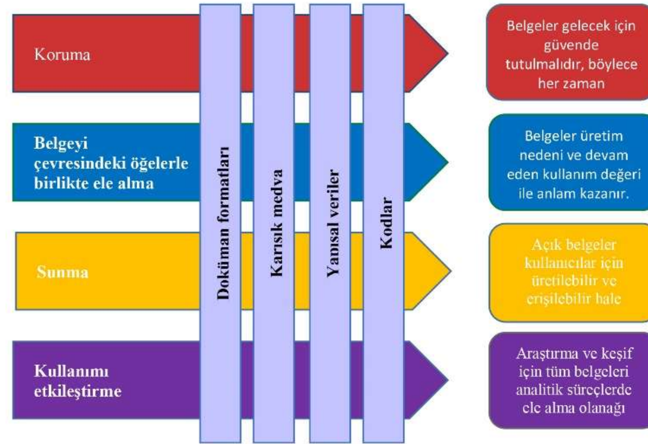
Değişimle birlikte karşımıza çıkan zorluklar ise Tablo1'de verilmiştir.

Değişim	**Zorluklar**
Dijital Dönüşüm	Alışık Olmadığımız Formatlar (basılı - elektronik)
Kullanıcılar (X,Y,Z, Alfa Kuşağı)	Kullanıcıları Anlama Arama Davranışlarındaki Değişim
Veri Patlaması	Dijitalleşme ile birlikte idari ve kültürel arşivlerde engel olamadığımız ve hızla büyüyen veri miktarı
Veri Çeşitliliği	Resmi belgeler ve eklerindeki farklı dosya biçimlerine erişim sorunu Web, sosyal medya, harici veri tabanları Kullanıcı verilerinin tutulması gerekliliği
Akan Veri	Veri kaybı ve güvenlik sorunlarına anında müdahale Kullanıcı sorunlarına anında müdahale

Tablo1. Arşivlerdeki Değişim ve Karşılaşılacak Zorluklar

Dijital teknolojiler, arşivlerin halk tarafından nasıl erişildiğini ve kullanıldığını da değiştirmiştir. Her ay milyonlarca ziyaretçi arşivlerin web sitelerini ziyaret etmektedir. Kullanıcıların, arşivlenen hükümet web sitelerine ulaşmak, kamunun eski sosyal medya iletilerini görüntülemek, hukuk ile ilgili içeriklere ulaşmak, arşivlerin kataloglarında detaylı arama yapabilmek gibi dijital arşiv hizmetlerine ihtiyaçları bulunmaktadır. Arşivlerden beklentiler bir hayli yüksek durumdadır ve örneğin mobil cihazların gittikçe artan kullanımına da ayak uydurma zorunluluğu bulunmaktadır. Sosyal medya platformları bize yeni arşivleme zorlukları getirmektedir ancak aynı zamanda yeni kullanıcılara ulaşmanın heyecan verici yeni yollarını sunmaktadır. Ayrıca koleksiyonlarımızı kataloglamayı geliştirerek kullanıcıların arşive katkıda bulunma biçimini değiştirme potansiyeli de bulunmaktadır (The National Archives, 2017, s. 2).

Bu değişimle birlikte Elektronik belge yönetimini Şekil1'de gördüğümüz dört başlıkta değerlendirebiliriz.



Şekil1: How the digital archive provides value? (The National Archives, 2017, s.7)

Doğan'ın (Doğan, 2015) çalışmasında ele aldığı kütüphaneler için büyük veri, elektronik belge yönetim merkezleri ve arşivler içinde aşağıdaki iki ana başlık altında ele alınabilir.

- Büyük verinin, sunulan hizmetlerin geliştirilmesi için kullanımı
- Büyük verinin bir veri kaynağı olarak arşiv sisteminde yer alması

Elektronik belge yönetim merkezleri ve dijital arşivlerde büyük verinin kullanım alanları ile ilgili aşağıdaki örnekler verilebilir.

1. Arşivciler, büyük veriyi kullanarak çoklu formattaki büyük miktardaki kayıtlara erişimi geliştirebilir. Veri ve metin madenciliği kullanan yapay zekalar ile arama özellikleri geliştirilebilir. Kullanıcıyı tanıyan sistemlerle, kullanıcıya özel sonuç getiren arama araçları kurulabilir. Bilgi erişim ve aramada kullanılan dil semantik bir yapıya dönüştürülebilir. Kullanıcı bilgilerinin eldeki kayıtlardan başka dış kaynaklardan, örneğin bazen diğer veri ambarlarından, bazen sosyal medya veri kaynaklarından elde edilebilmesi de önemlidir.
2. Kullanıcıların daha iyi tanınması konusunda ise, göz ve imleç hareketlerini izleme araçları gibi uygulamalarla arama araçları ve kullanıcı hizmetleri geliştirilebilir.
3. İç ve dış kaynaklardan toplanan (yani arşiv metinleri, kullanıcı kayıtları, sosyal medya verileri, web sayfalarından elde edilen veriler, vb.) verilerden elde edilen sonuçlar kurumsal kültürü yansıtacak; kurumun bir kültür arşivi yapısını ortaya koyacaktır. Bu durum, verilerin bir arşiv materyali gibi arşivlerimizde bulundurulması gerektiğinin bir başka nedenidir.
4. Bütün bu veriler arşive ait veri ambarında saklanmalıdır.
5. Yapılandırılmamış ve yapılandırılmış kayıtlar için içeriğin uygun metadata alanları ile nitelendirilmesi son derece önemlidir. Böylece büyük veri araçları kullanan araştırmacılar analiz yapmak için uygun çerçeveye sahip olacaktır
6. Toplanan verilerden hazırlanan veri setleri, kurumlar arası işbirliği sayesinde yapılacak bir düzenlemeyle bir veri havuzunda toplanabilir ve yetki, yasalar ve etik ilkeler doğrultusunda ortak kullanıma açılabilir.

Şüphesiz yukarıda sayılanlara daha fazlası da eklenebilir. Biz burada sadece belli başlı olanları vermeye çalıştık.

Belge Yönetim merkezleri ve Arşivler, Büyük Veri konusunda gelişme göstermek istiyorlarsa Doğan'ın (Doğan, 2015) çalışmasında kütüphaneler için ele aldığı gibi arşivcilerin ve belge yöneticilerinin de öncelikle aşağıdaki soruları vb. cevaplamalarında fayda vardır:

- Merkezlerinde hangi veriler, ne gibi şekillerde, nerelerde üretilmektedir?

- Bu veriler, başka hangi hizmetlerde kullanılabilir?

- Dışarıdan hangi veriler alınırsa, hangi hizmetlerimizi iyileştirmelere neden olabilir?

- Hangi veriler dış kaynaklardan arşiv sistemine eklenmelidir (Teknolojik kapasite ve kaynaklarımız bağlamında değerlendirilmelidir)?

- Dış kaynaklardan edinilen veriler, erişime sunulacak mıdır veya nasıl sunulacaktır ?

- Bu veriler hizmet verdiğimiz araştırmacılara nasıl bir katkıda bulunacaktır ?

- Bu verilerin toplanması, işlenip değerlendirilmesi yönündeki mevzuat ve etik yapı ne durumdadır?

Bu sorular daha fazla ayrıntıya inilebilecek niteliktedir. Bunun yanında her bir sorunun ayrı bir analiz ve değerlendirmeye tabi tutulması gerektiği de ortadadır.

Bilgi merkezlerinde çalışacak Bilgi Uzmanlarının büyük veri konusunda Stanton'ın (Stanton, 2012), kütüphaneciler için verdiği aşağıdaki disiplinler ile ilgili eğitim alarak, bu disiplinlerle ortak çalışma yapılabilecek duruma gelmeleri gerekmektedir. Bu disiplinleri Stanton (Stanton, 2012), aşağıdaki şekilde vermiştir:

- İstatistik

- Bilgisayar Programcılığı

- Veritabanı Yöneticiliği

- Grafik Tasarımcı

- İlgili diğer disiplinlere ilişkin konular

Bu disiplinler günümüzde büyük veri ile birlikte kütüphaneciler için olduğu kadar elektronik belge yöneticileri ve arşiv çalışanları, hatta daha genel olarak bütün bilgi merkezleri çalışanları için de önemli bir hale gelmiştir.

Sonuç

Dijitalleşme ve belgelerin elektronik ortama taşınması işi ile birlikte "Büyük veri" konusunda yapılacak çalışmalar pek çok kurumun kaçınılmaz olarak gerçekleştirmeleri gereken süreçler olarak karşımıza çıkmaya başlamıştır.

Bu durum büyük veriyi niteleyen hacim, hız ve çeşitlilik gibi konularının tamamında kendine yer bulacaktır.

Bu kaçınılamaz durum için, gerekli teknolojik donanım ve yazılım geliştirilmesinde milli Ar-Ge projelerine ihtiyaç bulunmaktadır ve bu projelerin devlet desteği ile yapılmasında büyük fayda vardır. Bu projelerin milli arşivler tarafından yürütülmesi, projelerin ve araştırmacıların milli arşivler tarafından desteklenmesi son derece önemlidir.

Büyük veri ile ilgili politikalar geliştirilmesi ve konunun etik boyutuna ilişkin yasal düzenlemenin oluşturulması gerekmektedir.

İlgili merkezlerde çalışacak bilgi uzmanlarına bu konuda lisans ve lisansüstü programlar, hizmet içi eğitim ve seminerler aracılığı ile eğitimler verilmelidir.

Bu alanda yapılacak olan çalışmaların bir an önce gerçekleştirilmesi arşivlerimiz ve elektronik belge yönetim merkezlerimiz açısından son derece önemlidir.

Yukarıda anlatılanlar değerlendirildiğinde arşivlerimiz ve belge yönetim sistemleri için yetkili kurulların ulusal çapta çalışmalar ve projeler yapmaları gerektiği, bu projeler öncesi ve/veya içinde mevcut durumun saptanması gerektiği, yine aynı bağlam ve kapsamda eğitim için gerekli destek ve önlemlerin alınması gerektiği ortadadır.

Kaynakça

Akpınar, H. (2014). Data Veri Madenciliği Veri Analizi. İstanbul: Papatya Yayıncılık Eğitim.

Arslantekin, Sacit. "Veri Madenciliği ve Bilgi Merkezleri." Türk Kütüphaneciliği 17.4 (2003): 369-380.

Cackett, D. (2013). Information management and big data, a reference architecture. Redwood Shores: Oracle Corporation. 10 01, 2017 tarihinde http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.398.7632&rep=rep1&type=pdf adresinden alındı

Davis, K., & Patterson, D. (2012). Ethics of big data: Balancing risk and innovation. Sebastopol: O'Reilly.

Diebold, F. (2012, 11 26). A personal perspective on the origin(s) and development of "big data": the phenomenon, the term, and the discipline. 10 01, 2017 tarihinde University of Pennsylvania web Sitesi: http://www.ssc.upenn.edu/~fdiebold/papers/paper112/Diebold_Big_Data.pdf adresinden alındı

Doğan, K. (2015). Büyük verinin üniversite kütüphaneleri açısından önemi ve kütüphane hizmetlerinde kullanımı: Ankara Üniversitesi Kütüphaneleri örneği. (Yayımlanmamış yüksek lisans tezi) Ankara Üniversitesi Sosyal Bilimler Enstitüsü,Ankara.

Doğan, K., & Arslantekin, S. (2016). Büyük veri: önemi, yapısı ve günümüzdeki durum. DTCF Dergisi, 56(1), 15-36.

E-ARK Project. (2017). 10 01, 2017 tarihinde E-ARK Project Web sayfası: http://www.eark-project.com adresinden alındı

Erl, T., Khattak, W., & Buhler, P. (2016). Big data fundamentals, concepts, drivers & techniques. Indiana: Arcitura Education Inc.

HM Government. (2015). Big data for law. 10 09, 2017 tarihinde legislation.gov.uk Web Sitesi: https://www.legislation.gov.uk/projects/big-data-for-law adresinden alındı

Johnson, J. E. (2012, 07/08). Big data + big analytics = big opportunity. FinancialExecutive, s. 50-53.

Laney, D. (2001, 02 06). 3D data management: Controlling data volume, velocity, and variety. (A. D. Strategies, Dü.) 09 10, 2017 tarihinde Gartner Web Sitesi: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf adresinden alındı

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (Mayıs 2011). Big data: The next frontier for innovation, competition and productivity. McKinsey Global Institute.

Monino, J.-L., & Sedkaoui, S. (2016). Big Data, Open Data and Data Development (3. b.). London: ISTE Ltd.

National Archive of Malaysia. (tarih yok). Guidelines on electronic records management: managing electronic records in the unstructured environment. 09 20, 2017 tarihinde National Archive of Malaysia Web Sitesi: http://www2.arkib.gov.my/borang/unstructured_eng.pdf adresinden alındı

Oğuzlar, A. (2011). Temel metin madenciliği. Bursa: Dora.

Prytherch, R. (2005). Harrod's librarians' glossary and reference book : a dictionary of over 10,200 terms (10 b.). Hampshire: Ashgate Publishing Limited.

Schönberger, V. M., & Cukier, K. (2013). Büyük veri - yaşama, çalışma ve düşünme şeklimizi dönüştürecek bir devrim (1. b.). (B. Erol, Çev.) İstanbul: Paloma Yayınevi.

Stanton, J. M. (2012, 07 16). Data science: what's in it for the new librarian? Information Space. 09 20, 2017 tarihinde http://infospace.ischool.syr.edu/2012/07/16/data-science-whats-in-it-for-the-new-librarian/ adresinden alındı

The National Archives. (2016). Traces through time. 09 17, 2017 tarihinde The National Archives Web Sitesi: http://www.nationalarchives.gov.uk/about/our-role/plans-policies-performance-and-projects/our-projects/traces-through-time/ adresinden alındı

The National Archives. (2017, 03). The National Archives digital strategy (March 2017). 09 08, 2017 tarihinde The National Archives Web sitesi: https://www.nationalarchives.gov.uk/documents/the-national-archives-digital-strategy-2017-19.pdf adresinden alındı

U.S. National Archives and Records Administration. (2014). 09 27, 2017 tarihinde U.S. National Archives and Records Administration Web Sitesi: https://www.archives.gov/files/about/plans-reports/strategic-plan/2014/nara-strategic-plan-2014-2018.pdf adresinden alındı

Açık Devlet Verisi: Türkiye'de Bakanlıkların ve Bazı Kurumların Hazır Olma Durumları Üzerine Bir İnceleme

Open Data: A Study on Readiness to Open Data of Selected Turkish Ministries and Institutions

Prof. Dr. Türksel KAYA BENSGHIR
TODAİE Öğretim Üyesi
BM-CEPA Üyesi (2014-2017)

Öz

Günümüzde devletler, siber alanda varlıklarını güçlendirmek üzere dijitalleşmekte ve açık devlete dönüşüm çalışmaları yürütmektedir. Devletler «açık devlet» olarak daha şeffaf, katılımcı ve iş birliği geliştirme ilkeleri üzerinde yeniden yapılanarak verilerin akışkanlığını önleyen nedenleri ortadan kaldıracak şekilde verinin gizlilik-mahremiyet ve etik çerçevelerini tanımlanarak yeniden kullanıma açmak üzere, açık veri strateji ve politika geliştirme ve uygulamalarına hız vermektedir. Açık veri uygulamalarıyla ülkeler, devletin ve kamu iş süreçlerinin açıklığını ve şeffaflığını arttırmak suretiyle devlet verisini kullananların yeni ürünler veya hizmetler geliştirilmesine izin vermek, kamu yararını yakalamak, araştırmacılar veya sivil toplum kuruluşları tarafından veri kullanımını sağlayarak kamuoyu tartışmalarını teşvik etmek gibi fırsatlar yakalamayı amaçlamaktadır. Birçok kamu kuruluşu, yenilikleri teşvik etmek için verilerini kamuoyuna açıyor ve sosyal medyayı benimsemektedir. Açık veri uygulamaları gerek kamuda gerek özel sektörde yeni iş modellerinin geliştirimesine bir altlık oluşturmaktadır.. Bu gelişmeler, açık veri sağlayıcıları ve kullanıcıları arasında konumlandırılan yeni, bilgi-kaynaklı olmayan iş modellerinin ortaya çıkarmaktadır (Keen, P. W. G., Qureshi, S. 2006). Bu modeller araşında tek yönlü iletişim odaklı uygulamalar, etkileşimli uygulamalar, bilgi toplayıcılar, karşılaştırma modelleri, açık veri depoları ve hizmet platformları sayılabilir(Janssen ve Zuiderwijk, 2014). Hem kamu hem de özel kuruluşların değer yaratmaya katkıda bulunduğu melez iş modellerini doğurmaktadır. Özellikle 2010'dan itibaren aralrında ABD, İngiltere, İspanya ve Avusturalya'nın bulunduğu bir çok ülke açık devlet ve açık veri strateji ve politikalar hayata geçirmekte ve verinin üretkenliğinden faydalanarak başta ekonomik olmak üzere sosyal ve kültürel alanda kamu yararını artırmaya dönük çalışmalar yürütmektedir. Ülkemizde de benzer çalışmalar henüz olgunluk aşamasına gelmese de başlamıştır. Bu çalışmada, ülkemizde açık veri konusunda yapılacak akademik ve uygulamaya dönük çalışmalara ışık tutmak üzere, 2019 ve sonrası için kurumsal stratejik planlarını ilan eden bazı bakanlıkların ve kurumların bu dönemleri kapsayan stratejik plan ve eylemleri, 2016 faaliyet raporları, mevcut mevzuatları ve 2017 yılı kurumsal mali durum ve beklentiler raporları üzerinden içerik analizi yapılarak politika ve mevzuat bağlamında açık veri konusunda hazır olma durumları irdelenecektir. Elde edilen bulgular ışında, ülkemizde

kurumların açık veri konusunda farkındalıklarını ve hazır bulunuşluluklarını artıracak öneriler sunulacaktır.

***Anahtar Kavramlar**: Açık Veri, Mevzuat, Hazır Bulunuşluk, Bakanlık, Açık Devlet, Türkiye.*

Abstract

Today, governments are digitizing to strengthen their cyber-scene assets and are engaged in transformations into an open state. Government are stepping up their open data strategy and policy development and implementation to open up reuse by defining the confidentiality, privacy and ethical framework of the data so that it will be restructured on more transparent, participatory and cooperative development principles as the "open government". By means of open data practices, countries, governments and the public are aiming to increase the transparency and transparency of their business processes, to allow the users of government data to develop new products or services, to catch public interest, to encourage public debate by providing data use by researchers or non-governmental organizations. Many public organizations open their data to promote innovation and adopt social media. These developments are driven by new, non-information-driven business models that are positioned among open data providers and users (Keen, P. W. G., Qureshi, S. 2006). These models include one-way communication-oriented applications, interactive applications, data collectors, comparison models, open data repositories and service platforms (Janssen and Zuiderwijk, 2014). Hybrid business models, both public and private, contributed to creating value. It has been seen that distinguishing between different types of open data users is critical in explaining different business models. Especially since 2010, many countries including USA, UK, Spain and Australia have been carrying out studies aimed at increasing the benefits of social and cultural - intellectual field, especially economical, by taking advantage of the productivity of open-state and open data strategies and policies. Similar studies have begun in Turkey, although it has not yet reached maturity level. In this context, many countries are engaged in studies aimed at increasing the benefits of social and cultural intellectual commerce, especially economic, through the use of open government and open data strategies and policies and taking advantage of the productivity of the data. Similar studies in our country are carried out even though they are not yet maturing. In this study, some of the ministries and institutions that declared their institutional strategic plans for 2019 and beyond, with the aim of shedding light on the academic and practical work to be done on open data in our country, 2016 annual reports, current legislation and the year 2017 institutional financial situation and expectations reports will be analyzed to determine the readiness of open data in the context of policy and legislation. In the course of the findings, recommendations will be presented to increase awareness and readiness of institutions about open data in Turkey.

***Key Concepts**: Open Data, Legislation, Readiness, Ministry, Open Government, Turkey.*

Giriş

Şeffaf, hesap verebilir yönetimlerde nitelikli kamu verilerinin kamuoyu ile gizlilik, mahremiyet ve fikri haklar güvence altına alınmak koşuluyla yönetimi giderek ülkelerin gündeminde daha fazla yer almaktadır.

Ülkeler açık veriyi tanımak ve açık verilerin yayınlanmasına yardımcı olmak üzere uluslararası işbirlikleri oluşturarak çeşitli çalışmalar yapmaktadır. Açık veri mevzuatının oluşturulması, standartların ortaya konulması, kurumsal bilgi alt

yapılarının teknik ve yönetsel olarak hazırlanması ve yönetimin tüm kademelerinde açık veri yönetimi, kullanımı ve değer yaratma konularında farkındalıkların yaratılması gibi çalışmalar bunlara örnek olarak verilebilir. Açık veri girişimini sürdürülebilir kılmak, açık verilerin ekonomik, çevresel ve sosyal etkilerini yönetmede yetkinlik kazanmak giderek daha önemli hale gelmektedir (Hammell, R. ,Perricos, C ve diğerleri, 2012).

Açık Veri Enstitüsü (ODI), kamuda organizasyonel değişimi uzun vadede açık veriyi destekleme ve sürdürme üzereine oturtma çalışmalarına yön vermektedir. Açık veri ile ilgili rehberler ve standartların çıkarılması ve ülkelere açık veri yönetiminde yol gösterilmesi dikkat çeken önemli gelişmelerdir.[1]

Açık veri uygulamalarıyla ülkeler, devletin ve süreçlerinin açıklığını ve şeffaflığını arttırmak suretiyle devlet verisini kullananların yeni ürünler veya hizmetler geliştirilmesine izin vermek, kamu yararını yakalamak, araştırmacılar veya sivil toplum kuruluşları tarafından veri kullanımını sağlayarak kamuoyu tartışmalarını teşvik etmek gibi fırsatlar yakalamayı amaçlamaktadır.

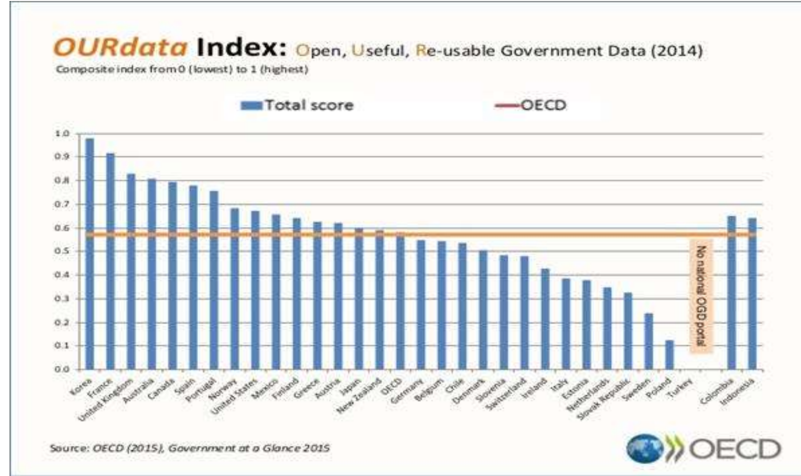
Literatürde kamu sektörü bilgileri (PSI), açık veri (open data-OD) açık devlet verisi (open government data-OGD) gibi kavramlarla karşılaşmaktayız. Özünde bu kavramlar veri varlıklarının akışkanlığını sağlayarak kamu yararını artırmada benimsenen yeni yaklaşımın kavramları olarak ortak özellik göstermektedirler. Açık devlet verisi kamu sektörü bilgilerinden farklı olarak sadece kamu verilerinin değil aynı zamanda sosyal medya verilerinin de kullanıma ücretsiz sunulmasını da kapsar (Europen Union, 2016).

OECD, Our Data 2014 indeksinde ülkelerin verilerini OUR-(O-Open, U-Usefulness, R-Reuse) kriterleriyle konumlandırmıştır (Şekil 1). G. Kore, Fransa, Birleşik Krallık, Kanada, İspanya ve Portekiz bu kriterlere sahip olmada 0.7 skorun üzerinde yer almaktadır. Türkiye Ulusal OGD Açık Devlet Veri Portalı olmayan ülke olarak yer almaktadır (OECD, 2017).

Web Foundation tarafından opendatabarometer.org adresinden yayınlanan Açık Veri Baro Metresi (Open Data Barometer) ülkelerin hesap verebilirlik, yenilikçilik ve sosyal etki için açık verileri nasıl yayınladığı ve kullandığının genel bir ölçüm aracı olarak hizmet sunmaktadır. 2017 Temmuz itibarıyla ülkelerin, açık veri barometredeki konumlarına baktığımızda 80 skorun üzerinde olan ülkeler arasında, Birleşik Krallık (100), Kanada (89,54), Fransa (85,13), ABD (81, 62), G. Kore (81,16) ve Avustralya (81,15) bulunmaktadır. Türkiye 36.88 değerle 50 skorun altında yer alan ülkeler arasında bulunmaktadır.

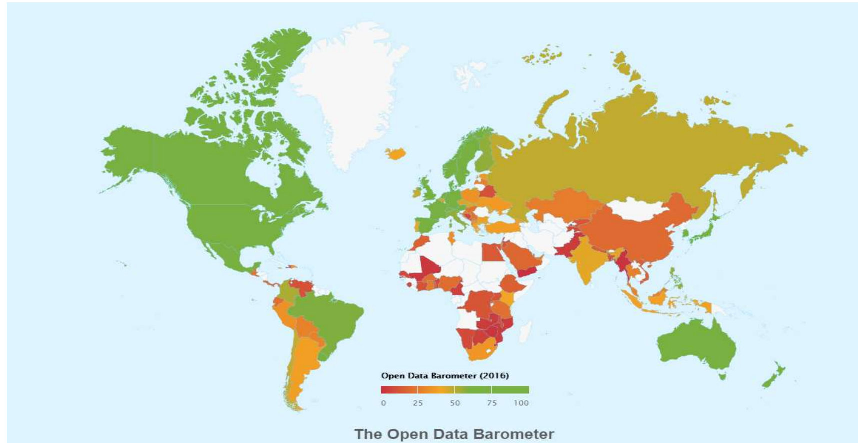
---

[1] https://theodi.org



Şekil 1. OECD, Our Data 2015 Açık, Faydalı Yeniden Kullanılabilir Kamu Verisi İndeks[2]

Türkiye'nin açık veri hazır bulunurluğu en fazla *vatandaş ve sivil haklar (53) boyutunda olup, iş dünyası ve işletmeler kategorisinde skoru 41, kamu politikasında 28, kamu faaliyetlerinde 24* dür. (World Wide Web Foundation, 2017) Şekil 2.

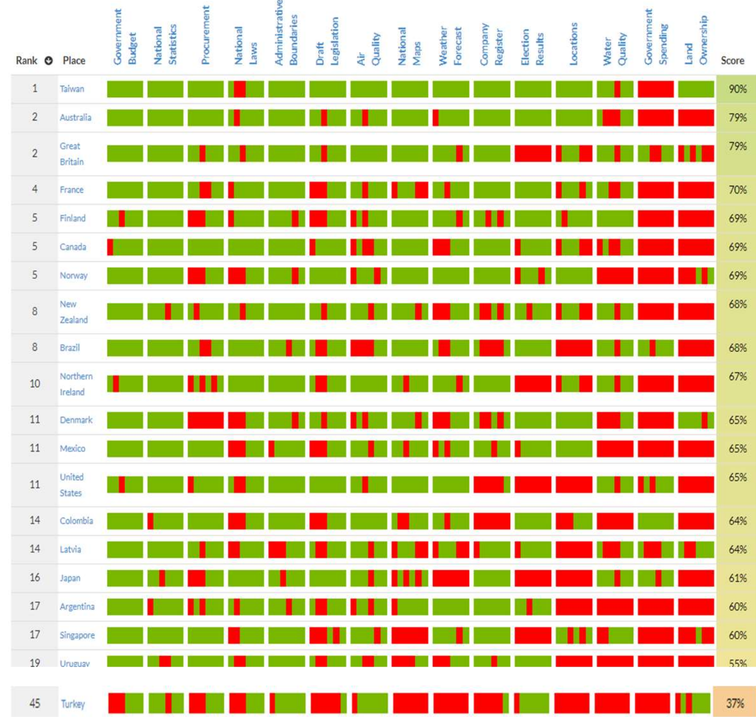


Şekil 2. Ülkelerin Açık Veri Barometredeki Konumları (2017, Temmuz)[3]

[2] OECD, 2017 «OECD Open Government Data project,» [Çevrimiçi]. Available:http://www.oecd.org/gov/digital-government/open-government-data.htm.[Erişildi: 07 07 2017]

[3] World Wide Web Foundation, «OpenDataBarometer,» [Çevrimiçi]. Available:http://opendatabarometer.org/?_year=2016&indicator=ODB. [Erişildi: 06 07.2017].

Ülkemizin halihazırda açık veri ile yaratılan etkiye baktığımızda 18 skor ile en fazla siyasal alanda etki yarattığı, bunu 10 skor ile sosyal alanı ve 7 skorla ekonomik alanı etkilediği görülmektedir. (World Wide Web Foundation, 2017). Özetle ülkemizde açık verinin kamuda gerek politika oluşturmada gerekse kamu faaliyetlerini etkin kılmada yetersiz uygulama düzeyinde olduğu gözlenmektedir. Bu veriler ışığında ülkemizde açık veri deneyiminde diğer bu alanda ilerleyen ülkelerle kıyaslandığında henüz başlangıç düzeyinde olduğu söylenebilir. Küresel açık veri indeksinde Tayvan, Avustralya, Birleşik Krallık, Fransa, Finlandiya, kanada ve Norveç başı çekmektedir. ülkemiz %37 skorla 45 sırada yer almaktadır. Şekil 3.



Şekil 3. Küresel Açık Veri İndeks[4]

Ülkemiz kurumsal bilgiler, ulusal istatistikler, hava kalitesi, seçim sonuçları ve tapu bilgilerini açık veri olarak sunmada daha iyi konumdalar. Buna karşın, ulusal haritalar, kamu harcamaları ve hava tahminleri alanlarında açık veri sunmada geri konumda olduğu gözlenmektedir Tablo 1.

[4] Global Open Data Index, https://index.okfn.org/place/ [Erişildi: 12.09.2017].

İyi Düzey	Orta Düzey	Zayıf Düzey
• İstatistik (TÜİK) • İdari bilgiler (Kamu kurumları web siteleri) • Hava kalitesi ve tahmin • Seçim sonuçları • Tapu bilgileri	• Bütçe • Tedarik • Yasa Taslağı hazırlama	• Ulusal harita • Su kalitesi • Kamu harcamaları • Lokasyon bilgileri

Tablo 1. Küresel Açık Veri indeksinde Türkiyenin Alanlar İtibarıyla Düzeyi

Bu çalışmada ülkemizde kamuda 2019 ve sonrası için kurumsal stratejik planlarını ilan eden bazı bakanlıkların ve kurumların bu dönemleri kapsayan stratejik plan ve eylemleri ile; 2016 faaliyet raporları, mevcut mevzuatları ve 2017 yılı kurumsal mali durum ve beklentiler raporları üzerinden içerik analizi yapılarak politika ve mevzuat bağlamında açık veri konusunda hazır olma durumları irdelenecektir.

Açık Devlet Verisine Kavramsal Bakış

Açık veri ve açık yönetim ile ilgili kavramların literatüre yönetişim olgunun yoğunlukla tartışıldığı son yıllarda girdiği gözlenmektedir. Özellikle e-devlet ve e-yönetişim çalışmalarıyla verilerin etkin yönetilmesinde kat edilen gelişmeler ülkelerin şeffaflık, hesap verebilirlik ve ekonomik değer yaratma hedefleri doğrultusunda en büyük kamu verisi üretici ve kullanıcısı olan kamunun bu alanda yeni kavram, yaklaşım ve modelleri anlaması ve içselleştiren çalışmalara gitmesi ihtiyaç olarak ortaya çıkmaktadır. Açıklığa kavuşturulması ve anlaşılması gereken yeni kavramlar arasında açık veri, açık veri ekosistemi, açık veri portalı, açık devlet/hükümet ve açık devlet/hükümet ortaklığı ve açık standartlar sayılabilir.

Açık Veri

Herkes tarafından herhangi bir yasal kısıt olmadan serbestçe kullanılmaya / tekrar kullanılmaya / yeniden dağıtılmaya izin veren "açık" bir lisans altında makine tarafından okunabilir biçimde halka açık olan verilerdir.

Açık Bilgi Toplumu Derneği «Open Knowledge Foundation» açık veriyi "Herhangi bir telif hakkı, patent ya da diğer kontrol mekanizmalarına tabi olmaksızın herkes tarafından ücretsiz ve özgürce kullanılan veri" olarak tanımlamaktadır (Open Knowledge International, 2017) .

Açık veri kullanılabilirlik, dağıtılabilir ve tekrar kullanılabilirlik olmak üzere üç temel olgu üzerinde ele alınmaktadır. Veri teknik ve hukuki olarak açık veri özelliği kazanır (Güngör, 2013). Teknik olarak açıklık, makineler tarafından okunabilen (machine-readable) standart yapıya uygunluğu ifade eder. Veri bilgisayar uygulamaları tarafından alınabilmeli ve anlamlı bir şekilde işleme tabi tutulabilmelidir. Yasal olarak açıklık ise, lisanslamayı ifade eder. Herhangi bir

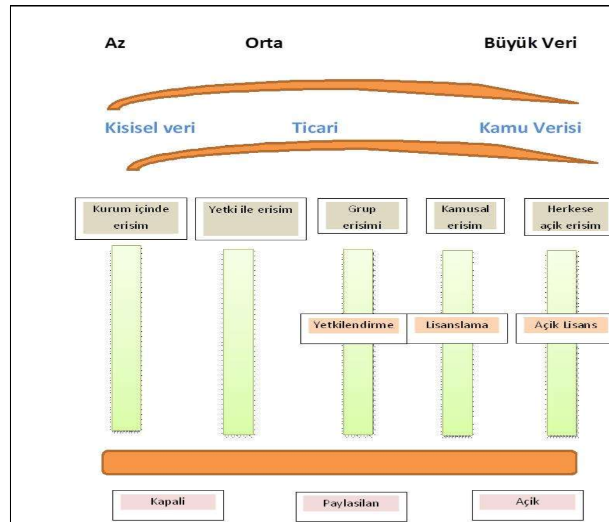
sınırlama olmaksızın, ticari ya da ticari olmayan kullanım ve tekrar kullanıma izin verilmesidir. Açık veri herkes tarafından kullanılabilir, dağıtılabilir, paylaşılabilir – kolay bulunabilir ve tanımlı –doğru ve güncel – standart bir formatta hesaplamaya uygun olmalıdır.

Açık verinin şu kriterleri taşıması beklenir:

• Eksiksiz • Öncelik • Zamanlılık • Erişilebilirlik • Ayrımcılık yapılmaması • Sürekli kullanılabilirlik, • Makine tarafından okunabilirlik • Açık standartlar / açık formatlar • Ücretsiz lisans • Varsayılan olarak açık • Zamanlı	• Kapsamlı • Kullanılabilir • Karşılaştırılabilir • Birlikte çalışabilir • İyileştirilmiş Yönetişim ve Katılım, • Kapsayıcı kalkınma sağlama • Yenilikçi

Açık Veri Spektrumu

Kamu verileri, hacim olarak azdan büyük veriye uzanan büyüklükten, kişisel nitelikten ticari ve kamusal niteliğe ve erişime kapalılıktan açık lisanslamayla herkese açık özellik taşıyabilir. Şekil 4.



Şekil 4. Veri Spekturumu
Kaynak. theodi.org/data-spectrum

Açık Veri Ekosistemi

Açık verilere yönelik bir yaklaşım, sadece liderlik, politika / yasal çerçeve, altyapıdan sorumlu kamu kurumlarını değil, aynı zamanda, ve kullanıcı topluluklarının durumu gibi diğer önemli aktörleri (geliştiriciler, üniversiteler, özel sektör, STK) de içerir.

Açık Veri Portalı

Kullanıcıların bir kamu, kurum ya da kuruluştan elde edilebilecek açık verilere erişimi için tek bir erişim noktası sağlanması.

En azından katalog olarak hareket eden bir platform (data.gov. sitesinin) oluşturulmasıdır.

Açık Hükümet

Şeffaf, hesap verebilir, katılımcı ve işbirliği ile çalışan devlet/hükümet

Açık Devlet/Hükümet Ortaklığı (OGP)

Devletler/Hükümetleri, hükümeti daha açık, sorumlu ve vatandaşlara duyarlı hale getiren küresel bir ortaklık. 2011 yılında kurulan OGP şu an 60'ın üzerinde üye ülkeye sahiptir.

Açık Standartlar

Kamuya açık olan, tescilli olmayan ve royalty-free olarak uygulanabilen teknik standartlar. Çoğu zaman açık standartlar, "açık" şeffaf bir süreçte geliştirilir ve bu sayede daha büyük bir grubun gelişimlerine katkıda bulunması sağlanır.

Ülkelerin ve kurumların açık verinin avantajlarından yararlanabilmeleri aşağıda sıralanan açık veri kritik faktörlerin yerine getirilmesine bağlıdır:

- Lider taahhüdü ve desteği
- Bilgiye erişim hakkı
- Açıklık- yetki ve sorumlukların belli olması
- Zamanlılık
- Kapsayıcılık – erişimde fırsat eşitliği ve çok kanallı erişim
- Kaynak yeterliliği (bilgi verme, danışma ve katılım için)
- Eşgüdüm
- Hesap verebilirlik
- Değerlendirme
- Aktif -katılımcı vatandaşlık.

Bu kritik faktörler ülkemizin açık veri politikasının oluşturulmasına da kapsamlı bir çerçeve sunmaktadır.

Açık verinin etkisi ve yarattığı ekonomik değerler ölçülmekte ve bu alanda yeni programlara girdi oluştururacak analizlere önem verilmektedir. Ancak bu alanda makro çalışmaların ekonomik etkiyi tahmin etmek için farklı göstergeler kullanması nedeniyle, hem mezo hem de mikro düzeyde etki çalışmaları eksiktir ve hesaplama yaklaşımları da farklılık göstermektedir. (Uhlir, 2009).

Bazı Ülkelerin Açık Veri Stratejileri ve Hedefleri

Ülkeler açık veri programlarını 2009' lardan itibaren geliştirmeye başlamışlardır. Bu amaçla farklı temel motivasyonlar çerçevesinde açık veri programları oluşturup çalışmalarını bu alanda sorumlu kurumlarda koordineli olarak yürütmektedirler Tablo 2' de Avusturalya, Danimarka, İspanya, Büyük Britanya ve ABD'de sürdürülen çalışmalar özetlenmiştir (Noor Huijboom, Tijs Van den Broek, 2017).

Ülke	**Program ve Yılı**	**Sorumlu Otorite**	**Temel Motivasyon**
Avustralya	Government response to the Gov 2.0 report, Open Gov declaration, 2010	AGIMO, 2010	Kamu sektörü bilgileri açık hale geldikçe ulusal varlıklar, olasılıklar – öngörmek, açık kamu verisi –PSI- ile yenilik yapmakve kamu yararını artırmak
Danimarka	"Open data Innovation Strategy ('Offentlige Data I Spil')", 2010	Bilim, teknoloji ve Yenilik BAkanlığı	Hükümet verilerine erişim, yeni hizmetler ve farklı analizler, yeni bilgiler ve vatandaşlara yararlı olan daha iyi bilgiler ve hem işletmeler hem de. BİT şirketleri dijital hizmetler geliştirmede yeni işler yaratmak ve kamusal verilere dayanan gelişmiş içerik ve vatandaşlar fikirleri ve yaratıcılığı pratik haline dönüştürmek ve günlük sorunlara çözümler üretmek.
İspanya	"Avanza2", 2010	Sanayi ve Turizm Ticaret Bakanlığı	"Veri, bilgi ekonomisi için çok önemlidir. Kamu verileri, yeni ürün ve hizmetlerin geliştirilmesiyle ekonomik değer üretilebilir. Ayrıca veriler vatandaşların katılımına ve demokratik hakların uygulanmasına ve elde edilmesine olanak tanır.
Büyük Britanya	Putting the Frontline First: Smarter Government, 2009	Hazine Müsteşarlığı, 2009	Eylem 1: vatandaşların ve yurttaşların rolünü güçlendirmek Toplum 1.3 Verileri radikal bir şekilde açma ve tanıtma şeffaflık: "Sonuçta daha bilgilendirilmiş bir vatandaş Daha yetkili bir vatandaş. Modern bir demokraside vatandaşlar,

			hükümetin nerede olduğunu göstermesini bekler Para harcanmış ve sonuç ne olmuştur. [...] Veri, aynı zamanda vatandaşlara ve işletmelere ekonomik yardımlar sağlamak El Değmemiş Girişim ve Girişimciliğin Serbest Bırakılması.
ABD	Open Government Memorandum and Plan, 2009	Beyaz Saray, 2009	Açıklık, demokrasiyi güçlendirecek, verimlilik ve etkinlik getirecek. Şeffaflık hesap verebilirliği artacak ve Hükümet faaliyetleriyle ilgili vatandaşlara bilgi sunulacak.

Tablo 2. Ülkelerin Açık Veri Stratejileri ve Hedefleri

Türkiye'de Açık Devlet Verisinin Politika ve Stratejik Çerçevesi

Türkiye'nin Açık Devlet Platformuna (OGP) üyelik süreci Eylül 2011 tarihinde başlamıştır. Bu kapsamında 2012 yılında bir eylem planı hazırlanmıştır. 2013 yılı Ağustos ayında da OGP'nin Türkiye'de uygulanmasına yönelik 2013/9 sayılı ve "Açık Yönetim Ortaklığı Girişimi" konulu Başbakanlık Genelgesi yayımlanmıştır (Resmi Gazete, 2013) [5]. Türkiye'nin birinci eylem planında verdiği taahhütler şu şekildedir:

- www.saydamlik.gov.tr ismiyle bir web portalı kurulması bu portal aracılığıyla şeffaflık, dürüstlük, hesap verebilirlik ve yolsuzlukla mücadele konularına ilişkin çalışmaların paylaşılması ve tüm vatandaşların bilgiye daha şeffaf ve açık bir şekilde erişmesi,
- Vatandaşların politika yapım ve uygulama süreçlerine aktif katılımının sağlanması için www.duzenleme.gov.tr ismiyle bir web portalı kurulması,
- www.harcama.gov.tr ismiyle bir web portalı kurularak kamu harcamalarında şeffaflığın sağlanması,
- Kamuda Şeffaflık ve Açıklık Danışma Platformu oluşturulması.

Birinci eylem planı ile ilgili çalışmaların başarı ile yürütülmesi için gerekli workshop, seminer ve konferansların düzenlenmesi ve bu konuda kamuoyunda farkındalık yaratılması öngörülmüştür. Bu kapsamda,

- ✓ Bürokratik engellerin azaltılması,
- ✓ Yolsuzlukla mücadelenin etkinliğinin anket gibi çalışmalar aracılığıyla ölçülmesi ve

[5] 52013/9 sayılı ve "Açık Yönetim Ortaklığı Girişimi" konulu Başbakanlık Genelgesi: http://www.resmigazete.gov.tr/eskiler/2013/08/20130823-8.htm.

✓ Elektronik ihale yapılmasını sağlayacak bir sistemin pilot uygulamalarının gerçekleştirilmesi.

Bu süreç içerisinde Türkiye birinci eylem planını hazırlamıştır. Ancak Türkiye, ikinci eylem planını hazırlaması gerektiği süreçte herhangi bir çalışma yapılmamıştır. Geçen sürede mevcut taahütleri gerçekleştirmede geciken ülkemiz Eylül 2017 itibarıyla bu platformada yer almamaktadır.

Türkiye'de Ulusal eDevlet Strateji Planı (2016-2019) ve BTS-Bilgi Toplumu Strateji Planında (2015-2017) açık veriye yer verilmiştir. Strateji dokümanında açık veri ile ilgili şu hedefler dikkat çekmektedir:

- BTS 50 nolu eylem, Kültürel ve Bilimsel Nitelikte Sayısal Bilgiye Açık Erişimin Sağlanması
- BTS 67 nolu eylem, Kamu Verisinin Paylaşılması

Ayrıca, ülkemizde yürürlüğe koyulan 2015-2018 İstatistiki Bilgi Altyapısının Geliştirilmesi Programı (Resmi İstatistik Programı (RİP[6]) kapsamında) TÜİK ve diğer kurum ve kuruluşlarca yayınlanan tüm istatistikleri tek bir çatı altında toplayan bir internet portalı (RİP Portalı) kurularak işlerliği sağlanacağından söz edilmiştir. Öte yandan, 2015-2018 Yerelde Kurumsal Kapasitenin Güçlendirilmesi Programında veriye toplanıp kullanılacak istatistikler olarak bakılarak, "belediyelerin sistematik veri toplaması ve kamuoyu ile paylaşması sağlanacaktır." hedefi konulmuştur.

Ulusal e-Devlet Stratejik planında (2016-2019) açık veri uygulamasıyla beklentiler şöyle ifade edilmiştir:

"Verilerin açık veri olarak paydaşların kullanımına açılması ile bir taraftan kamu yönetiminde şeffaflık ve güçlendirilmekte, diğer taraftan ekonomik değer yaratılmakta ve kamu hizmetlerinde nicelik ve nitelik bakımından iyileştirmeler sağlanmaktadır.

Ayrıca açık veri yaklaşımlarıyla şeffaflık ve hesap verebilirliğin güçlendirilmesi katılımcılığın etkinliğini de artırmaktadır".

Bu ifade kamuda açık veri uygulamaların kamu yönetiminde şeffaflık ve hesap verebilirlik ilkelerinin yerine getirilmesine katkı vermesinin yanı sıra hizmet üretme ve sunmada etkinlik-iyileştirme getirmesi ve katılımcılığın sağlanmasına zemin oluşturması beklenmektedir.

2016-2019 Ulusal e-Devlet Stratejik planında açık veri hedefi, iki temel çerçeveye oturtulmuştur. Bunlardan birincisi, açık veri paylaşım portalinin oluşturulması (data.gov.tr), ikincisi ise, kamu verilerinin açık veriye dönüştürülmesi ve paylaşılmasıdır.

---

[6] http://www.tuik.gov.tr/Kitap.do?metod=KitapDetay&KT_ID=0&KITAP_ID=302.

Planda Hedef 4.2 başlığında "Açık Verinin Kullanım Alanları Yaygınlaştırılacaktır. Türkiye'de açık veri konusunda kamu kurum / kuruluşlarının yanında özel sektör, sivil toplum kuruluşları gibi diğer paydaşları da içine alacak şekilde yapılacak çalışmaların çerçevesinin çizilmesi, kriterlerin belirlenmesi ve kullanımının yaygınlaştırılması sağlanacaktır." İfadesine yer verilerek açık veri olgusunun kamu kesiminin yanı sıra özel sektör ve STK'ları da kapsayacağının altı çizilmiştir.

Bu eylemden sorumlu ve ilgili kurum ve kuruluşları Başbakanlık (S), Ulaştırma Denizcilik ve Haberleşme Bakanlığı, TÜİK, TÜBİTAK, Üniversiteler, Özel Sektör, Sivil Toplum Kuruluşları, Kamu Kurum ve Kuruluşları (Veri Paylaşım Standartlarının Belirlenmesinde Görev Alacak Merkezi Yönetim Birimleri ve Yerel Yönetimler) olarak yer almıştır. Bu eylemin, 01.07.2016 başlaması ve 31.12.2017 da tamamlanması planlanmıştır. Bu eylemin uygulama adımları,

- "açık veri paylaşım portali ihtiyaçları belirlenmesi,
- diğer ülkelerin açık veri konusundaki çalışmaları incelenmesi,
- veriyi kullanacak paydaşlar çalışmaya dahil edilecek, özel sektör ve vatandaşların da açık veri konusunda ihtiyaçları belirlenerek, talep odaklı çalışmalar yürütülmesi ve açık veri paylaşım portali oluşturulması." olarak sıralanmıştır.

Hali hazırda çalışmalar sürdürülmektedir. 12-13 Ekim 2017 tarihinde Başbakanlık'da Türkiye açık veri portal hazırlığına altlık oluşturmak üzere açık veri çalıştayı yapılmış, konuyla ilgili uzmanların görüşleri alınmıştır.

Türkiye'de Bakanlık ve Bazı Kamu Kurumların Açık Veri Uygulamasında Hazır Olma Durumları

Ülkemizde Ulaştırma, Denizcilik ve Haberleşme Bakanlığından çıkarılan ve 3 Eylül 2016 tarihinde yayınlanan E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik (Resmî Gazete Sayı : 29820) ile kamu kurumlarında veri paylaşım ilkesi açıklığa kavuşturulmuştur. Buna göre E-Devlet Hizmetlerinin Sunulması İlkeler MADDE 5 ı) bendinde "*Kamu kurum ve kuruluşlarınca oluşturulan ve işlenen elektronik ortamdaki verilerin, kaynakların verimliliğinin sağlanması ve mükerrerliğin önlenmesi ilkeleri çerçevesinde katma değerli hizmetler yaratmak üzere mer'i mevzuattan kaynaklanan istisnalar saklı kalmak kaydıyla paylaşılması*" ifadesine yer verilmiştir. [7]

Aynı yönetmelikte MADDE 7 – (1) e-Devlet hizmetlerinin kapsamı ve yürütülmesinde kamu kurum ve kuruluşlarının görev ve sorumlulukları arasında "*Mer'i mevzuattan kaynaklanan istisnalar saklı kalmak kaydıyla, e-Devlet hizmetlerinin yürütülmesi kapsamında ilgili veriler, kamu kurum ve kuruluşları*

[7] http://www.resmigazete.gov.tr/eskiler/2016/09/20160903-2.htm (9.9.2017)

arasında yapılan protokoller çerçevesinde elektronik ortamda paylaşılır ve ilgili kullanıcılara sunulur" denilmektedir. Bu düzenleme veri paylaşımını protokollere bağlamaktadır. Türkiye her ne kadar 2012 yılında OGP platformuna katılıp açık veri çalışmalarını taahhüt etmiş se de bu düzenleme de açık veri perspektifi bulunmadığı görülmektedir.

Öte yandan, Maliye Bakanlığı 16 Mayıs 2017'de Bütünleşik Kamu Mali Yönetim Sistemi Genelgesini yayımlayarak mevcut veri tutarsızlıklarını ortadan kaldıracak bir mali bilgi alt yapısı tesis etmek üzere çalaışma yürütmektedir. Bütünleşik Kamu Mali Yönetim Bilişim Sistemi projesi başlatarak bu çalışmayla bütçe kanunu hazırlıklarının başlatılmasından kesin hesabın TBMM'de kanunlaşmasına kadar geçen mali işlemlere ilişkin süreçlerde kullanılan otomasyon sistemlerinin, elektronik belge, elektronik imza, otomatik muhasebe gibi yeni teknolojik imkanlara kavuşturulması ve mali yönetim sistemini için süreç odaklı bütünleşik bir bilişim sistemi altyapısına dönüştürülmesi amaçlanmaktadır.[8]

Kamuda güvenlikli veri iletişimi sağlamak üzere KamuNet KamuNet (Kamu Sanal Ağı) oluşturuldu. Bu ağ ile kurumlar arası veri iletişimi internete kapalı olan daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi ve oluşturulması, planlanan ortak veri merkezi/merkezlerinin dahil edilmesi amaçlanmıştır[9].

Bu genel açıklamalara ilave olarak ülkemizde bakanlık ve kamu kurumlarının açık veri uygulamalrına hazır bulunuşluğu üst düzey sahiplik, yasal düzenlemeler, Kurumlar arası veri paylaşımı, Veri/bilgi Yönetiminden sorumlu Bakanlık ve Kamu Kurumlarının Stratejik Planlarında Açık Verinin/ Kamu Verisinin Yeri ve başta Ulaştırma Haberleşme ve Denizcilik Bakanlığı Stratejik Planı 2014-2018 olmak üzere ilgili diğer kurumların (Kalkınma Bakanlığı, Maliye Bakanlığı, Tüik ve SGK stratejik plan ve eylemlerinde açık veri politikasının ne ölçüde dile getirilmiş olduğu incelenmiş ve bulgular aşıda özetlenmiştir:

Üst Düzey Bilişim/Bilgi Yöneticisi (CIO) Atama ve Yetkilendirme

Ülkemizde Türkiye'nin dijital dönüşümünden sorumlu bilişim yöneticisi kadrosu inşaa edilmemiştir. 2011 yılında yürürlüğe giren 655 sayılı Kanun Hükmünde Kararname (KHK) ile e-Devlet politikalarına yönelik görev ve sorumluluk Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na (UDHB) verilmiştir. Bakanlık bünyesinde kurulan e-Devlet Hizmetleri Dairesi Başkanlığı e-Devlet çalışmalarını yürütmektedir.[10] Bakanlık ve diğer kamu kurum ve kuruluşlarında

[8] https://www.csb.gov.tr/db/strateji/editordosya/BKMYBS%20(Web).pdf 7.10.2017.
[9] http://www.udhb.gov.tr/doc/siberg/KamuNetweb.pdf (10.4.2017).
[10] http://www.edevlet.gov.tr/e-devlet-hakkinda/ (10.4.2017).

henüz üst düzey veri/bilgi yöneticisi kadrosu bulunmayıp dijital dönüşüm bilgi işlem başkanlık/daire/şubelerince yürütülmektedir.

Yasal Düzenlemeler

Türkiye'de veri ve bilgiye ilişkin mevcut düzenlemeler olarak,

- 5846 Fikir ve Sanat Eserleri Kanunu (1951)
- 25269 Bilgi edinme hakkı kanunu (2003)
- 5429 Sayılı İstatistik Kanunu (2005)
- 6698 Kişisel verileri Koruma Kanunu (2016)
- Diğer kanunlar ve düzenlemeler içinde konuyla ilgili düzenlemeler sayılabilir.

Kurumlar arası veri paylaşımı

Kurumlar diğer kurumlarla aralarında yaptıkları protokollerle veri paylaşımlarını,

- forumlar
- yazışmalar
- bilgi sistemleri
- web servis teknolojileri
- taşınabilir Medya ortamlara
- VPN
- public Cloud servis
- upload link gibi araçlar, platformlar ve mekanizmalarla yürütmektedir.

Kamuda veri paylaşımı sağlıklı dijitalleşme modelinin bir parçası olarak değil palyatif bir çözüm yoluyla işleyen araya KEP ve KEP hizmeti veren kurumsal yapıların girdiği dolaylı bir yapılanmayla gerçekleştirildiği gözlenmektedir.

Veri/bilgi Yönetiminden sorumlu Bakanlık ve Kamu Kurumlarının Stratejik Planlarında Açık Verinin/ Kamu Verisinin Yeri

Çalışmada veri/bilgi paylaşımda doğrudan sorumlu kurumların kurumsal stratejik planlarında açık verinin izi aranmıştır.

Ulaştırma Haberleşme ve Denizcilik Bakanlığı Stratejik Planı 2014-2018

Planda açık veri kavramı hiç yer verilmemiştir. Ancak veri kavramı 13 defa geçiyor. Veriye ilişkin şu vurgular yer alıyor:

- Veri tabanı kurulması
- Veri sunumunda güveniğin sağlanması
- Veri entegrasyonu
- Veri kritik alt yapılarını belirlemek

2015 faaaliyet raporunda ise veri güvenlği, CBS ve veri yönetimi ve verilerin tek pencereden sunulması konuları geçmektedir. Açık veri kavramı yer almamıştır.

Kalkınma Bakanlığı 2014-2018

Planda açık veri kavramı hiç yer verilmemiştir. Kamu verisi kavramı yer alıyor. "2014-2018 Dönemi Bilgi Toplumu Stratejisi ve Eylem Planının öngördüğü Kullanıcı Odaklı e-Devlet Hizmet Sunumunun Sağlanması, Kamu Bilişim Tedarikinin Etkinleştirilmesi, Kamu Verisinin Paylaşımı ve Kamu Politikalarının Oluşturulmasında BİT Destekli Katılımcılık Programı Geliştirilmesi eylemleri kapsamında ortaya konacak politika, yasal düzenleme ve araçların uygulamaya geçirilmesinde Bakanlık öncü rol oynanacaktır."

Temel değerler arasında "uzmanlığı, bilgiyi ve öğrenmeyi esas alma ve veriyi bilgiye dönüştürme" sayılmaktadır. Diğer kurumlarla entegre bilgi sistemlerinin tesis edilmesi ihtiyacı vurgulanıyor.

Maliye Bakanlığı 2013-2017 Stratejik Planı

Planda açık veri kavramı hiç yer verilmemiştir.

TÜİK 2017-2021 Stratejik Planı

Planda açık veri kavramı hiç yer verilmemiştir. Kamu versi geçmiyor. Veri kavramı 279 kez geçiyor. TÜİK Başkanı Plan sunuşunda "*Türkiye İstatistik Sistemindeki tüm verilerin karşılaştırılabilirliğini ve tutarlılığını temin etmek, üretilen tüm verilerin entegrasyonu temel hedeflerimiz arasındadır*." söylemi dile getirilmiştir.

SGK

Planda açık veri kavramı hiç yer verilmemiştir. Kamu verisi hiç geçmiyor. Bilgi sistemi kavramı mevzuat bilgi sistemi olarak 5 kez geçmektedir. SGK'nın son yıllarda gerçekleştirdiği dijital uygulamalardan bazıları şunlardır [11]

- İlaç işlemlerini tek bir uygulama üzerinden yürütebilmek amacıyla MEDULA Eczane, Doktor, Optik (e-Reçete) uygulaması getirilmiştir.
- Vatandaşların sağlık hizmetlerinden faydalanmalarını kolaylaştıracak Sağlık Provizyon Aktivasyon Sistemi (SPAS) uygulaması getirilmiştir.
- Hastalık, iş kazası, doğum yapma, yol yardımı, tıbbi malzeme ödemeleri gibi konularda artık kurum içi vezneler kaldırılarak Mali Otomasyon Sistemi Projesi (MOSİP) tahsilat sistemi üzerinden bankalarla anlaşmalı olarak yapılabilir hale getirilmiştir.
- Devlet memurlarının emeklilik işlemlerinin kolaylaştırılması ve kısaltılması ile ilgili "HİTAP Projesi" uygulamaya konulmuştur.

[11] www.sgk.gov.tr/

- İşverenlerin sosyal güvenlik işlemlerini kolaylaştırıcı e-bildirge ile e-Borcu Yoktur uygulaması getirilmiştir.
- Vatandaşın sevk işleminden doğan yolluk ve gündelik ödemelerini daha hızlı ve kolay alabilmesi amacıyla e-Sevk projesi hazırlanmıştır.
- Sağlık hizmet sunucularının ilaç kullanım raporlarının elektronik ortamda kayda alınması amacıyla e-Rapor ve devam reçetesi uygulaması geliştirilmiştir.
- Sosyal güvenlik sistemini daha çağdaş standartlarda yürütülmesi amacıyla 1 Ekim 2017 tarihi itibariyle elektronik fatura uygulamasına geçilmiştir.

Açık Veri Politikasının Uygulanmasına İlişkin Sorunlar

Açık veri ile karşılaşılan en önemli sorun henüz açık verinin ne olduğu, önemi bilgi ekonomisindeki sinerjik getirisi ve Türkiye Bilgi Toplumu Stratejik Plan 2015-2018 ve Türkiye eDevlet Stratejik planı 2016-2019 da yer lana açık veriye ilişkin amaç ve hedefler konusunda bilgi ve farkındalık eksikliğinin olmasıdır.

Açık kavramı kurum yetkililerini endişelendirmekte olup gizlilik ve mahremiyet ve güvenlik zaafiyeti getirebileceği konusundaki beklentileri konuya sıcak bakmalarına engel oluşturmaktadır.

Kamu veri olgusu yeterinde önem verilmediği, veri alanında uzmanlaşma, kurumsal yapı, CIO gibi yönetici pozisyon vb eksikliği dikkat çekmektedir.

Kamu kurumları veri alanında hem kendi alt yapılarını dijitalleştirme hem de diğer kurumlarla entegre veri paylaşım konusunda sorunlar yaşamaktadır. Veri paylaşım sorunlarının önündeki teknik yönetsel ve davranışsal/kültürel engeller bulunmaktadır.

Gerek kamu gerek diğer sektörlerde sağlıklı bir dijital arşiv yönetimi de henüz sağlanamamıştır.

Kamuda çok aktörlü yönetim anlayışının (yönetişim) yerleşmemiş olması açık veri ile ilişkisinin henüz tam oturtulamamış olması da bir eksiklik olarak dikkat çekmektedir. Elektronik yönetişim ve açık yönetim anlayışı içinde açık verinin bir politika olarak benimsenme ihtiyacı vardır.

Açık veriye dayalı kamu politikasını ve hizmet sunumunu iyileştirme ve bilgi ekonomisini güçlendirme hedefleri ancak her düzeyde dijital beceri ve yeteneklerin geliştirilmesine bağlıdır. Ülkemizde dijital beceri tabanı olşturacak politika ve uygulamalara ihtiyaç bulunmaktadır.

Kurumların veri yönetim yeteneklerini ve veri yönetim alt yapılarını iyileştirecek politika ve mekanizmalarda eksiklikler bulunmaktadır. Özellikle kurumsal web

sitelerinde veri yönetim ve sunum konusunda başta standartlaşma, güncellik, erişilebililirlik ve gizlilik, etik ve güvenlik konularında sıkıntı olabilecek eksiklikler bulunmaktadır.

Sonuç ve Öneriler

Dijitalleşmeyle beraber veri paylaşılarak sağladığı doğurganlığın farkına varan kurumlar her türlü kamusal veriyi paylaşma ve birlikte çalışabilir konuma gelme konusunda yönetsel ve hukuksal alt yapılarını yenileştirme arayışına girmektedir. Bilgi endüstrilerinin büyümesine koşut olarak daha iyi işleyen bir kamu idaresi, daha şeffaf ve etkin işleyen yönetim arayışı bu beklentilerin katalizörü olan veri yönetimini de daha kritik hale getirmektedir. Güvenlik, gizlilik ve mahremiyetin güvence altına alınacağı bir veri yönetimi özellikle kişisel verilerin korunmasını güvence altına alan bir yaklaşımın kamuya tesis edilmesi ihtiyacını da doğurmaktadır. Nitekim kurumlar veri koruma ve paylaşma yönergeleri çıkararak bu alanın mevzuat alt yapısını tesis eden uygulamalara öncelik vermektedirler.

Bununla birlikte, teknolojik gelişmeler ve artan miktarda kamuya açık veriler, kişisel olmayan ve kişisel veriler arasındaki çizgiyi bulanıklaşmaktadır. Açık veriler, özellikle anonim veya toplu haldeyken ilk bakışta kişisel veriler gibi görünmeyebilir. Bununla birlikte, onu halka açık diğer verilerle birleştirerek veya anonimleştirilmediğinde kişisel veriler haline gelebilir. Bu konuda kamuda titiz bir ortak anlayış geliştirme ihtiyacı vardır. Çoğu ülke bu çalışmalara dayanarak açık veri çalışmalarını meşrulaştırmış olsa da birçok politika yapıcı, açık verilerin ülkeleri ve belirli sektörler ya da kuruluşlar üzerindeki kesin ekonomik etkisinin büyük ölçüde belirsiz kaldığını da kabul etmektedir.

Öte yandan ülkelerin gizlilik düzenlemeleri verilerin kişisel veri konumuna dönüşmesine neden olabilir ve açık veri uygulama alanlarını daraltıcı bir konuma götürebilir (Kulk, S. ve Loenen, B. V. 2012). Gizlilik ve açıklık dengesinin sağlanması ülkede kapsamlı ve bütüncül bir bakış açısı ile dijitalleşme sürecinin yürütülmesini gerekli kılmaktadır.

Ülkemizde açık verinin sosyal kültürel ve ekonomik değer yaratabilmesi için temelleri 2003 de atılan 2023 vizyonuna uygun bir Dijital Türkiye Strateji ve ajandası oluşturulmasına ihtiyaç vardır. Dijital Türkiye 2023 Strateji çalışmasında aşağıda listelenen hususlar dikkate alınmalıdır:

- Stratejinin odağını iletişim, etkileşim ve paylaşım kısaca bilişime dayandırmalı,
- Bilişimin gücü yönetim değil ağ yönetişimi ile taçlandırılarak açık veriye/bilgiye dayalı bir bilgi ekonomisinin motoru olacak şekilde toplumun tüm kesimlerini kapsayacak bir dijitalleşme yol haritası oluşturulmalı,
- Ülkenin diğer makro plan ve politika belgelerin bunlarla uyumlaştırılmalıdır.

Kaynakça

Güngör, V. G, 2013 «E-Devlet ve e-Dönüşüm,». [Çevrimiçi].: https://ece581.files.wordpress.com/2013/11/ece581-ac3a7c4b1k-veri-ac3a7c4b1kdevlet.pdf. [Erişildi: 02 06 2017].

Hammell, R., Perricos, C., Lewis, H., Branch, D. (2012). Open growth. Stimulating demand for open data in the UK Deloitte analytics.London, England:Deloitte.Google Scholar

http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN046727.pdf

Keen, P. W. G., Qureshi, S. (2006). Organizational transformation through business models. A framework for business model design.Paper presented at the the 39th Hawaii International Conference on Information Systems, Koloa, Kauai, HI. Google Scholar. http://ieeexplore.ieee.org/abstract/document/1579713/ .

Kulk, S., Loenen, B. V. (2012).Brave new open data world? International Journal of Spatial Data Infrastructures Research, 7,196–206.Google Scholar

https://repository.tudelft.nl/islandora/object/uuid:66d1f3a0-644f-4fe7-87d0-adcd7515a91f?collection=research.

Noor Huijboom, Tijs Van den Broek 2017, "Open data: an international comparison of strategies", [Çevrimiçi] http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN046727.pdf, 12. 08. 2017.

Open Knowledge International, 2017 «What is Open?,» [Çevrimiçi].

https://okfn.org/opendata/. [Erişildi: 16 5 2017].

Rob Kitchin , 2014, The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Concequences, https://books.google.com.tr/books?hl=tr&lr=&id=GfOICwAAQBAJ&oi=fnd&pg=PP1&dq=open+data&ots=pdrcTU_iTW&sig=vuGesw4kKBLnXMrQBrktw_iAf1g&redir_esc=y#v=onepage&q=open%20data&f=false.

Uhlir, P.F. (2009). The Socioeconomic Effects of Public Sector Information on Digital Networks: Toward a Better Understanding of Different Access and Reuse Policies: Workshop Summary, US National Committee CODATA, in cooperation with OECD.

Ubaldi, B. (2013). Open government data: Towards empirical analysis of open government data initiatives. OECD Working Papers on Public Governance: No. 22. Paris, France:OECD.Google Scholar. https://search.proquest.com/openview/eae0dba100f69321171cd0682e350182/1?pq-origsite=gscholar&cbl=54503.

Zuiderwijk, A., Janssen, M., Choenni, S., Meijer, R., Sheikh_Alibaks, R. (2012).Socio-technical impediments of open data. Electronic Journal of eGovernment, 10,156–172. Google Scholar

available online at www.ejeg.com

Diğer Kaynaklar

BTS-Bilgi Toplumu Strateji Planında (2015-2017), [Çevrimiçi].http://www.bilgitoplumustratejisi.org/tr/doc/8a9481984680deca014bea4232490005 [Erişildi: 28.09 2017].

European Commission. (2011). Digital agenda: Commission's open data strategy, questions & answers. Retrieved March 25, 2013.

http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/891&format=HTML&aged=1&language=EN&guiLanguage=en Google Scholar.

European Union, 2016 «Open Data Goldbook for Data Manager and Data Holders,» [Çevrimiçi]. https://www.europeandataportal.eu/sites/default/files/goldbook.pdf.

Global Open Data Index, https://index.okfn.org/place/ [Erişildi: 12 09.2017].

OECD, 2017 «OECD Open Government Data project,» [Çevrimiçi].http://www.oecd.org/gov/digital-government/open-government-data.htm.[Erişildi: 07 07 2017].

World Wide Web Foundation, «OpenDataBarometer,» [Çevrimiçi]. Available: http://opendatabarometer.org/?_year=2016&indicator=ODB. [Erişildi: 06 07 2017].

OECD, «OECD Open Government Data project,» [Çevrimiçi]. Available: http://www.oecd.org/gov/digital-government/open-government-data.htm. [Erişildi: 07 07 2017].

Resmi Gazete, 2013 «52013/9 sayılı ve "Açık Yönetim Ortaklığı Girişimi" konulu Başbakanlık Genelgesi:,» 2013. [Çevrimiçi]. http://www.resmigazete. gov.tr/eskiler/2013/08/20130823-8.htm. [Erişildi: 02 07 2017].

theodi.org/data-spectrum.

Ulusal eDevlet Strateji Planı (2016-2019) ,». [Çevrimiçi].http://www.edevlet.gov.tr/wp-content/uploads/2016/07/2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf [Erişildi: 22 09 2017].

World Wide Web Foundation, 2017, «Open DataBarometer,» [Çevrimiçi]. http://opendatabarometer.org/?_year=2016&indicator=ODB. [Erişildi: 06 07.2017].

2. BÖLÜM

YENİ TEKNOLOJİLER, GÜVENLİK VE HUKUK

Elektronik Yazışma Projesi Güvenlik Katmanları ve Uygulama Geliştirme Esnasında Dikkat Edilmesi Gereken Hususlar

Electronic Correspondence Project Security Layers and Considerations During Application Development

Dr. Vural ÇELİK
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
Dr. Tamer ERGUN
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
Erhan TURAN
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
Serpil SALDIK
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
Merve Melis BALKAYA
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
Meltem SEYİRT
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi

Öz

Elektronik işlem hacminin önemli bir noktaya geldiği ve sürekli büyümeye devam ettiği günümüzde kurumların süreçlerini elektronik ortamda yürütmesi ve bu sebeple elektronik belge yönetim alt yapısı kurması hiç kuşkusuz önem arz etmektedir. Genel itibariyle ülkemizdeki devlet kurumları da bu doğrultuda hareket etmekte ve süreçlerini elektronik ortama hızla taşımaktadır. Bu kapsamda yapılan elektronik dönüşümün bir sonraki adımı ise, kurumların kendi bünyelerinde oluşturdukları elektronik belge yönetim sistemlerinin birbirleriyle konuşur hale gelebilmesidir. Ortak çalışabilirlik adı verilen bu eylem, kurumların resmi yazışma ihtiyaçları kapsamında gerekli olan tüm bileşen ihtiyaçlarını karşılamalı ve bunlara ek olarak kimlik doğrulama, bütünlük, inkar edilemezlik ve gizlilik gibi bilgi güvenliğine dair tamamlayıcı mekanizmaları da sağlamalıdır. Elektronik Yazışma Projesi, elektronik ortamda yapılan kurumlar arası yazışmalarda, ihtiyaç duyulan resmi yazışmalara ait bileşenleri sağlayan ve aynı zamanda kurumlar arası ortak çalışabilirliği oluşturmak hedefiyle hayata geçirilmiş bir proje olarak günümüze gelmiştir. Bu projenin sağlıklı çalışabilmesi ve yaygınlaşabilmesi için çağımızda önemi bir tehdit haline gelen ve elektronik verilerin ele geçirilmesi, değiştirilmesi gibi tehditlere sebebiyet veren güvenlik ataklarına karşı dayanıklı olması gerekmektedir. Elektronik Yazışma Projesinde kurumların bu tehditlere karşı dayanıklılık sağlayabilmesi adına elektronik imza, elektronik mühür ve şifreleme katmanları kullanılabilmektedir. Belirtilen

güvenlik katmanları tehditlere karşı dayanıklılık adına projede sunulmaktadır fakat bu katmanları uygulama düzeyinde gerçekleyecek geliştiricilerin de güvenlik öğelerine belli düzeyde hakim olması uygulamanın sağlıklı çalışması açısından önem arz etmektedir. Geliştiricilerin milli ürünler kullanması ve bu ürünlerin uygulamalara entegrasyonu aşamasında açık kapı bırakmayacak önlemleri alması gerekmektedir. Bu özellikler göz önünde bulundurularak gerçekleştirilen uygulamaların uluslararası standartlara uygunluğu 2017/21 Sayılı Başbakanlık Genelgesi'nde belirtildiği üzere TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi (Kamu SM) tarafından yapılacak ve onaylanan kurumlar Kamu SM web sitesinden yayımlanacaktır. Kurumların uygulamalarını Kamu SM'nin yapacağı ilgili değerlendirme olumlu sonuçlanana kadar kullanmaması güvenlik açısından önemlidir.

Anahtar sözcükler: *Elektronik Yazışma Projesi, Elektronik Yazışma Paketi, Elektronik İmza, Elektronik Mühür, Kriptografi*

Abstract

As electronic transaction volume has reached a significant point and continues to grow steadily, it is undoubtedly important for institutions to carry out their processes in electronic environment and for this reason to establish an electronic document management infrastructure. In general, the state institutions in our country are moving in this direction and they are carrying their processes rapidly to electronic environment. The next step in the process of electronic transformation in this context is that the electronic document management systems that institutions create in their own bodies can become communicated with each other. This action, called interoperability, must meet all the component needs that are required by the institution's formal correspondence needs and provide complementary mechanisms for information security such as authentication, integrity, non-repudiation and confidentiality. The electronic correspondence project has come to be a project that has been passed through with the aim of establishing the necessary components of official correspondence in the inter-institutional correspondence made in the electronic environment and at the same time creating the interoperability between the institutions. In order for this plant to be able to function and spread in a healthy way, it must be resistant to security attacks, which are a major threat in our day, and cause threats such as the seizure and alteration of electronic data. In the Electronic Correspondence Project, electronic signature, electronic seal and encryption layers can be used for the institutions to provide resistance against these threats. The specified layers of security are presented in the project in the name of resistance to threats, but it is important for the developer to implement these layers at the application level as well as for the healthy operation of the application to have some degree of control over the security elements. Developers need to take precautions not to leave open doors while integrating these products into applications and also using national products is highly recommended. Institutions that will be evaluated in compliance with international standards and approved by TÜBİTAK BİLGEM Governmental Certification Authority (Kamu SM) will be published on the Kamu SM website. The evaluation task is given to Kamu SM as stated in the Prime Ministry Circular No. 2017/21. It is important for the safety of the institutions not to use their applications until be informed about the positive evaluation done by Kamu SM.

Keywords: *Electronic Correspondence Project, Electronic Correspondence Package, Electronic Signature, Electronic Seal, Cryptography*

Giriş

5070 sayılı elektronik imza kanunuyla birlikte hukuki olarak tanımlanan ve o dönemden itibaren yavaş yavaş e-dönüşüm kapsamındaki süreçlere dahil edilen elektronik imza mekanizması, günümüzde ıslak imzanın yerini büyük oranda almaktadır (Kanun, 2004). Bu geçiş sürecinde kurumlar daha çok kendi süreçlerine odaklanmış, resmi yazışmalarla ilgili usül ve esaslara tabi bileşenlerin elektronik ortamdaki karşılıklarını bulmakla ilgili kendi bünyelerinde çalışmalar yapmış ve yine buldukları çözümleri iç işleyişlerine dahil etmişlerdir fakat gelinen noktada haberleşme ihtiyacının sınırları genişlemektedir.

Küreselleşen dünyamızda bilgisayar ağlarının yayılması birçok kolaylığı da beraberinde getirmiştir. Bireylerin hizmet alacakları varlıklara uzaktan erişimi, cihazların kendi aralarındaki ve bireylerle olan haberleşmesi, iletişim mekanizması olarak mobil cihazların kullanılması hayatımıza fazlasıyla girmiş bulunmaktadır. Kurumların kendi işleyişlerini elektronik ortama taşıması her ne kadar bu alışkanlığın bir örneği veya destekleyicisi olsa da asıl varılması gereken nokta, kurumların sadece kendi içlerinde değil diğer kurumlarla elektronik haberleşebilmesidir. Bu haberleşmenin doğal olarak, bilinen ve genel yöntemlerin üstünde, kurumların ihtiyaçlarına yönelik resmi yazışmalarla ilgili usül ve esaslarda tanımlanan bileşenleri içeren spesifik kuralları da beraberinde taşıması gerekmektedir. Bunun yanında bahsetmiş olduğumuz elektronik evrimleşme her ne kadar hayatımızı kolaylaştırmış olsa da bir taraftan haberleşme esnasında iletilen bilginin güvenliği hususunda önlem alma ihtiyacını da beraberinde getirmektedir. Bilgi güvenliği denilince akla ilk gelen öğeler bilginin bütünlüğü, kaynağının doğrulanması, inkar edilememesi ve gizliliğidir. Haberleşme esnasında belirtilen bilgi güvenliği öğelerinden bazıları veya hepsi ihtiyaca yönelik kullanılmaktadır. Dolayısıyla kurumlar arası elektronik yazışmayla ilgili üretilecek çözüm belirtilen bilgi güvenliği ihtiyaçlarını da adreslemelidir.

Elektronik Yazışma Projesi belirtilen bu ihtiyaçları karşılamak adına temelleri 2010 yılında atılmaya başlanmış, Kalkınma Bakanlığı sorumluluğunda ve birçok kurumun desteğiyle hayata geçirilmiş resmi yazışma projesidir. Bu proje kapsamında kurumlarla görüşülerek yazışmalarla ilgili ihtiyaçlar belirlenmiş ve belirlenen ihtiyaçlar doğrultusunda bir ortak çalışabilirlik rehberi hazırlanmıştır (Rehber, 2016). Rehber'de ortak çalışabilirlik kuralları yanında bilgi güvenliğiyle ilgili kullanılabilir güvenlik mekanizmaları da tanıtılmıştır. Bu mekanizmalar sırasıyla elektronik imza, elektronik mühür ve şifrelemedir. E-imza ve e-mühür genel itibariyle veriyle ilgili kimlik doğrulama, bütünlük ve inkar edilemezlik özelliklerini sağlarken, şifreleme ise gizlilik özelliğini sağlamaktadır. Belirtilen mekanizmaların e-Yazışma Paketi (EYP) verisinin hangi bölümüne ve hangi sırayla uygulanacağı teknik rehberde anlatılmaktadır.

Bu çalışmamızda, bir kurumdan diğer bir kuruma gönderilecek olan EYP verisinin oluşturulması aşamasında uygulanacak güvenlik mekanizmalarının

özelliklerinden ve sağladıkları katkılardan bahsedilmektedir. Bunun yanında EYP uygulaması geliştiricilerin ve bu uygulamaları devralacak kurum uzmanlarının dikkat etmesi gereken hususlardan bahsedilmektedir. Bu kapsamda birinci bölümde güvenlik mekanizmalarının temelini oluşturan kriptografik öğelerle ilgili temel bilgilerden, ikinci bölümde güvenlik mekanizmalarının EYP verisiyle olan ilişkisinden ve üçüncü bölümde ise geliştirme aşamasında dikkat edilmesi gereken hususlardan bahsedilmektedir.

Tanımlar

Kriptoloji

Kriptoloji, şifreleme ve şifre çözme bilimidir. Kriptoloji, verilerin belirlenen yöntemlere göre şifrelenmesi, hedefe iletilmesi ve iletilmiş şifreli verilerin çözülmesiyle ilgilenmektedir. Kriptoloji; kriptografi ve kriptoanaliz olmak üzere ikiye ayrılmaktadır. Kriptografi şifrelemeyle, kriptoanaliz ise şifre çözme ve analizle ilgilenmektedir.

Kriptografi, bilgilerin gizli tutulmasını sağlamak için kullanılan tekniklerin tümüdür. Kriptografi, verileri yetkisiz kişilerce okunamayan bir biçimde dönüştürmekte ve verilerin şifreli biçimde iletilmesini sağlamaktadır. Şifreli veriler yetkili kişideki anahtar kullanılarak çözülmektedir. Böylelikle güvenli iletişim sağlanmış olur.

Bilgi güvenliğinin birçok kolunda kriptografi kullanılmaktadır. Şifreli veri, şifrelemede kullanılan anahtar olmadan asla çözülemez. Bilgiler, şifreli biçimde iletilirken ve depolanırken bütünlüğü korunmaktadır. Kriptografi ayrıca inkar edilemezlik prensibinin sağlanmasına da yardımcı olmaktadır. Şifreleme sistemleri için en önemli dört bileşen aşağıda detaylandırılmaktadır. Sistemler bu bileşenlerden bir veya daha fazlasını sağlayabilmektedir.

Kimlik Doğrulama: Şifreleme sistemleri kullanılarak uzaktaki bir kullanıcının veya sistemin kimliği doğrulanabilmektedir. Yaygın olarak kullanılan Güvenli Soket Katmanı (SSL) ve elektronik imza buna örnek gösterilebilir. İmzanın ilgili kişi tarafından oluşturulup oluşturulmadığı ya da kullanıcının doğru sunucuya bağlanıp bağlanmadığı elektronik sertifika ile teyit edilmektedir (ITU-T X.509, 1997).

İnkar Edilemezlik: İnkar edilmezlik kavramı, e-devlet, finans ve e-ticaret uygulamaları için özellikle önemlidir. Kriptografik yöntemler, kişinin ilgili işlemi yaptığını kanıtlamak için gereklidir. Kriptoloji sayesinde, kişinin işlemi kendinin gerçekleştirdiğini inkar etmesi engellenebilmektedir. Örneğin, bir müşteri, başka bir hesaba transfer talebinde bulunabilir ve daha sonra, hiçbir talepte bulunmadığını iddia ederek paranın hesaba iadesini isteyebilir. Bu senaryoda işlemler kriptografi kullanılarak gerçekleştirilmişse, işlemin kişi tarafından

yapıldığının ispatı mümkün olmaktadır. Kişinin işlemi daha önce kendine resmi olarak tahsis edilmiş ve yalnızca kendisinde bulunan bir anahtarla yaptığı ispat olarak kullanılabilmektedir. Bu ispatın geçerliliği, ilgili anahtarın kişiye güvenilir makamlarca tahsis edilmesi ile sağlanmaktadır.

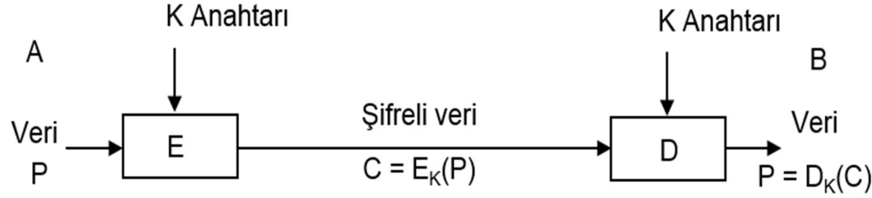
Gizlilik: Kriptografinin sağladığı en önemli bileşenlerden biri de gizliliktir. İlgili verinin istenildiği takdirde gizli bir biçimde saklanabilmesi veya iletilebilmesi son derece önemlidir. Şifreleme sistemlerinin en temel görevi gizlilik prensibini sağlamak olarak görülebilir. Sistemin gizlilik prensibinin sağlanması, şifreli verinin yalnızca yetkili tarafça çözülebildiğinin garanti altına alınmasına bağlıdır. Eğer veri güçsüz algoritma ve/veya anahtarlar kullanılarak şifrelenmişse gizlilik tehlikeye girmektedir.

Bütünlük: Kriptografi, verilerin gizli bir biçimde aktarılmasının yanında, aktarım sırasında değiştirilmemesini sağlamak için de kullanılabilmektedir. Veriyi gönderen taraf, veri ile birlikte gönderdiği kriptografik değer ile alıcı tarafın bütünlüğünü kontrol etmesini mümkün kılmaktadır. İlgili değer yalnızca yetkili tarafça oluşturulabilecek bir anahtar ile hesaplanmaktadır. Böylelikle araya giren saldırgan veri üzerinde fark edilmeksizin değişiklik yapamamaktadır.

Kriptografi için çeşitli algoritma türleri bulunmaktadır. Kriptografi, simetrik ve asimetrik olarak iki temel kola ayrılmaktadır.

Simetrik Kriptografi

Simetrik kriptografi, kriptografinin en geleneksel şeklidir. Simetrik şifreleme sisteminde, ilgili taraflar ortak ve tekil bir anahtarı paylaşmaktadır. Paylaşılan anahtar kullanılarak veriler şifrelenmekte ve şifreli veriler yine aynı anahtarla çözülmektedir. Simetrik algoritmalar, asimetrik algoritmalara göre genelde daha hızlıdır ancak ilgili taraflar arasında simetrik anahtarın paylaşımı ek yöntemler kullanılmadığı takdirde problem olmaktadır. Simetrik anahtara sahip taraf, söz konusu anahtarı kullanarak şifrelenmiş mesajlar oluşturabilmekte ve o anahtarla şifrelenmiş mesajların şifresini çözebilmektedir. Şekil 1'de gösterildiği gibi Kullanıcı A, Kullanıcı B'ye veri göndermek istediğinde, K anahtarını kullanarak veriyi şifrelemekte ve şifreli veriyi göndermektedir. Kullanıcı B kendisinde bulunan aynı K anahtarını kullanarak şifreli veriyi çözmektedir. Bağımsız ve güvenli iletişim kanalları kurmak isteyen taraflar her oturumda farklı anahtar kullanmalıdır ve kullanılan anahtarların rastgele seçilmesi önem arz etmektedir. Bu durum sistemde çok sayıda anahtar olmasına sebep olmaktadır. Anahtarları dağıtma ve yönetme zorluğu sebebiyle simetrik kriptografi genellikle tek başına tercih edilmemektedir.



Şekil 1. Simetrik Kriptografi

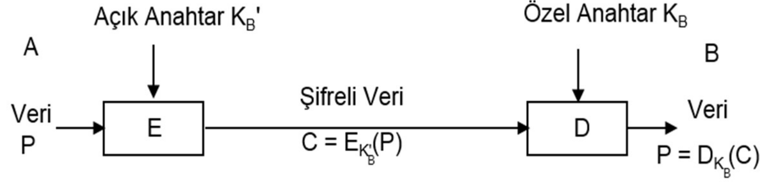
Veri Şifreleme Standardı (DES), 3DES ve Gelişmiş Şifreleme Standardı (AES) en çok tanınan simetrik algoritmalardır. DES 56 bitlik karmaşıklık sağlayan anahtarlar kullanmaktadır. Bu anahtarlar gelişen teknoloji ile zayıflamış ve 3DES kullanılmaya başlanmıştır. 3DES algoritması ise DES algoritmasının arka arkaya 3 kez uygulanmasıyla oluşturulmakta ve 112 bitlik karmaşıklık sağlamaktadır. Teknolojinin hızla gelişmesi 3DES'den daha güçlü algoritma arayışları başlatmış ve Amerika Birleşik Devletleri Standartlar ve Teknoloji Enstitüsü (NIST) yeni bir algoritma için yarışma düzenlemiştir. Bu yarışmayı Rijndael yani bilinen adıyla AES algoritması kazanmıştır. Çoğu uygulama için, 3DES şu an için kabul edilebilir derecede güvenlidir ancak yeni uygulamalar için AES kullanılması önerilmektedir.

Asimetrik Kriptografi

Asimetrik kriptografide, herkes tarafından erişilebilen açık anahtar ve yalnızca sahibinin erişiminde olan, açık anahtara matematiksel olarak bağlı özel anahtar olmak üzere bir anahtar çifti kullanılmaktadır. Asimetrik kriptografi hem şifreli mesajlaşmada hem de elektronik imzada yaygın biçimde kullanılmaktadır. Diffie Hellman, RSA (Rivest-Shamir-Adleman), ElGamal ve Eliptik Eğri en çok kullanılan algoritmalardır.

Şekil 2'de gösterildiği gibi Kullanıcı A, Kullanıcı B'ye veri göndermek istediğinde, Kullanıcı A, Kullanıcı B'nin açık anahtarına erişmektedir. Veri daha sonra bu anahtarla şifrelenmekte ve Kullanıcı B'ye gönderilmektedir. Kullanıcı B'nin açık anahtarı ile şifrelenmiş iletiler, yalnızca Kullanıcı B'nin özel anahtarıyla çözülebildiği için güvenli şekilde iletişim sağlanmaktadır.

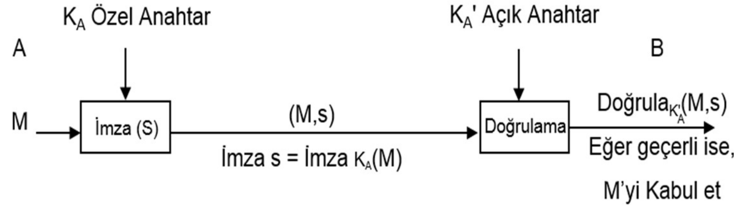
SSL asimetrik şifrelemeye bir örnektir. SSL protokolünde simetrik şifreleme ve asimetrik şifreleme birlikte kullanılmaktadır. Öncelikle istemci ve sunucunun katkısı ile simetrik anahtar bileşenleri oluşturulmakta ve asimetrik şifreleme ile simetrik anahtar paylaşılmaktadır. Sonrasında trafik simetrik şifreleme ile sürmektedir.



Şekil 2. Asimetrik Kriptografi

Asimetrik kriptografinin en yaygın kullanım alanlarından biri de elektronik imzadır. Sistemdeki Güvenlik Katmanları bölümünde elektronik imza detaylı olarak anlatılmaktadır.

Şekil 3'de Kullanıcı A, Kullanıcı B'ye bir mesaj ve mesajın kendisinden geldiğine dair bir kanıt göndermek istemektedir. Bunu gerçekleştirmek için Kullanıcı A, mesajı özel anahtarıyla şifrelemektedir. Bu şifreleme işlemi elektronik imza olarak adlandırılmaktadır. Mesaj bu noktadan sonra yalnızca Kullanıcı A'nın açık anahtarı kullanılarak çözülebilmektedir. Bu durum, Kullanıcı A'nın ilgili iletiyi oluşturduğunu garanti etmektedir. İlgili senaryonun sağlanması için açık anahtarın Kullanıcı A'ya ait olduğu garanti altına alınabilmeli ve işlem sırasında ispatlanabilmelidir. Açık anahtarın ilgili kişiye ait olduğunu ispatlayan veriye Elektronik Sertifika denir. Elektronik sertifikalar, Elektronik Sertifika Hizmet Sağlayıcılar (ESHS) tarafından verilmektedir.



Şekil 3. İmza Oluşturma ve Doğrulama

Özet Fonksiyonları

Özet fonksiyonları her uzunlukta veriyi girdi olarak alabilmektedir ve matematiksel fonksiyonlar yardımıyla temelde bu girdiye özel sabit uzunlukta özet değerleri oluşturmaktadır. Özet alma işlemi son derece hızlı yapılabilen bir işlemdir. Güvenli bir özet alma işleminde verinin özeti hızlı bir biçimde oluşturulabilirken özetten aynı şekilde veriye geri dönmek, istenen özete sahip bir başka anlamlı veri üretmek pratikte mümkün değildir. Belirli bir özete karşılık gelecek veriyi oluşturmanın, özet değeri değişmeyecek şekilde veri ile oynamanın ve aynı özete sahip iki farklı mesaj bulmanın (çarpışma) pratikte imkansız olması özet fonksiyonlarının sağladığı ana prensiplerdir.

Mesaj Özet Algoritması-5 (MD-5), Güvenli Özet Algoritması-1 (SHA-1) ve Güvenli Özet Algoritması-2 (SHA-2) en çok bilinen özet algoritmalarıdır. MD-5 özet fonksiyonunun sağlaması gereken ana prensipleri artık sağlamadığı ve manipülasyona açık olduğu için güvensiz bir algoritmadır. SHA-1 algoritmasında birçok çarpışma bulunduğu için, bu algoritma da zayıf olarak görülmektedir. Uygulamalarda SHA-256, SHA-384 veya SHA-512 algoritmalarının kullanılması önerilmektedir.

Sistemdeki Güvenlik Katmanları

Elektronik İmza

Elektronik imza, 15 Ocak 2004 tarihli 5070 Sayılı Elektronik İmza Kanununda, "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanmıştır (Kanun,2004). Elektronik imzanın sağladıkları mesajın bütünlüğünün korunması, kaynağın doğruluğunun ispatlanması ve inkar edilemezliktir. Elektronik imza temelde asimetrik kriptografiye dayanmaktadır. Elektronik imza oluşturmak için belgenin matematiksel özet değeri hesaplanır ve bu değer imza sahibinin özel anahtarıyla şifrelenir. İmzayı doğrulamak isteyen taraf imzalanan belgenin özet değerini hesaplar ve imza içerisinde belirtilen özet değeri ile karşılaştırır. İmzalanan belge üzerinde bir değişiklik olması durumunda özet değerleri tutmayacaktır. Böylece belgenin bütünlüğü garanti altına alınmış olur. İmzayı doğrulamak isteyen taraf, imza sahibinin açık anahtarına ihtiyaç duyar. İmza sahibinin açık anahtarla ilişkilendirilmesi elektronik sertifikayla sağlanmaktadır. Böylelikle imzayı atan kişi bu imzayı attığını inkar edemez ve belgenin kaynağı doğrulanabilir.

Elektronik ortamda oluşturulan imzaların kanuni açıdan ıslak imzayla aynı hükmü taşıması için güvenli elektronik imza olarak oluşturulması gerekmektedir. 5070 sayılı kanunda güvenli elektronik imza, "Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza" olarak tanımlanmıştır (Kanun, 2004). Güvenli elektronik imza oluşturulabilmesi için Türkiye'de bu hizmeti vermeye yetkili ESHS'den nitelikli elektronik sertifika (NES) temin edilmelidir.

İmza oluşturma öncesinde ve imza doğrulama işlemi sırasında, sertifika geçerliliğinin kontrol edilmesi gerekmektedir. Sertifika geçerlilik kontrolleri sırasında imza sahibinin sertifikasının ve güven zincirindeki tüm ESHS sertifikalarının geçerlilik ve iptal kontrolleri yapılmalıdır. Ayrıca imzanın atıldığı zamanı belirten zaman damgası bilgisinin geçerlilik kontrolü yapılmalıdır. Tüm bu kontroller sırasında elde edilen verilere doğrulama verileri denir.

Elektronik İmza Formatları

ETSI TS 101 733 standardında farklı kullanım alanlarının ihtiyacını karşılayacak imza tipleri belirlenmiştir (ETSI TS 101 733, 2013). Basit Elektronik İmza (BES) minimum özelliklere sahip imza tipidir. İçerisinde imzanın oluşturulma tarihini güvence altına alan, kanuni yönden geçerli zaman bilgisi bulunmamaktadır. Zaman Damgalı Elektronik İmza (ES-T), temelde BES imzayı kapsayan ve bunun yanında kanuni olarak imzanın oluşturulduğu tarihe işaret eden zaman damgası bilgisini içeren imza tipidir. Zaman damgası ile imzanın oluşturulma zamanı güvence altına alınır. Elektronik imzanın uzun süre geçerliliğini koruması için imzanın uzun dönemli olarak doğrulanabilmesine imkan tanıyan Genişletilmiş Uzun Elektronik İmza (ES-XL) tipi tanımlanmıştır. ES-XL imza, temelde ES-T imza üzerine kurulmuştur. ES-T imzadan farklı olarak içerisinde sertifika doğrulama verileri bulunmaktadır. Böylelikle imza doğrulama için dışarıdaki herhangi bir sisteme bağlanıp doğrulama verilerinin edinilmesine gerek kalmaz; doğrulama için gereken tüm verilere imza dosyasının içeriğinden erişilir. Bir diğer uzun dönemli elektronik imza olan Arşiv Elektronik İmza (ESA), temelde ES-XL imza tipi üzerine arşiv zaman damgası alınmasıyla oluşturulmaktadır. ESA, e-imzalı belgelerin imza doğrulama verilerinin geçerlilik süresinden daha uzun bir süre saklanması gerektiği durumlarda kullanılmalıdır.

NES'ler, ESHS'ler tarafından belirli standartlar çerçevesinde üst kurulun denetiminden geçerek üretildiğinden, genel itibariyle sistemlerde sertifika bazında uyumsuzluk bulunmamaktadır. Ancak sistemlerde bu sertifikalarla oluşturulan güvenli elektronik imzalar, farklı standartlar temel alınarak ve farklı imza tipleri tercih edilerek üretildiğinden sistemler arası birlikte çalışabilirliğin sağlanması güçtür. Bu konuda ortak bir standart belirlenmesi adına Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 2010 yılında "Elektronik İmza Kullanım Profilleri Rehberi" yayımlanmıştır. Bu rehberde P1, P2, P3 ve P4 olmak üzere dört farklı imza profili tanımlanmıştır. Tanımlanan imza profillerinde P1, temelde BES imzaya; P2, ES-T imzaya; P3 ve P4 ise uzun dönemli imzalara karşılık gelmektedir. Bu profiller temel alınarak oluşturulan imzaların içerisinde elektronik imza politikalarına uygun olarak üretildiklerine dair bilgiler yer almaktadır.

e-Yazışma Projesi ve Elektronik İmza

5070 sayılı kanun ve ilgili mevzuat ile elektronik imzanın belli şartları sağlaması durumunda ıslak imzayla eşdeğer kabul edilmesi, özel merasime tabi olmayan belgelerin elektronik ortamda yasal olarak imzalanmasını mümkün kılmaktadır. Bu durum, kurumların belge süreçlerini elektronik ortama taşımasına imkan sağlamaktadır. Kurumsal dokümanların üretilmesi, dağıtılması, imzalanması, arşivlenmesi ve tasfiye edilmesi Elektronik Belge Yönetim Sistemleriyle (EBYS) sağlanmaktadır.

Kamu kurumlarında EBYS'lerin yaygınlaşması ve Elektronik İmza Kanunu ile elektronik belgelerin hukuki değer kazanması sonucunda kurumlar arası

yazışmaların elektronik ortama taşınması gündeme gelmiştir. Ancak, söz konusu elektronik belgelerin diğer kamu kurum ve kuruluşları ile paylaşımı konusunda, birlikte çalışabilirliğin sağlanması için ortak bir yapıya ihtiyaç duyulmaktadır. Bu ihtiyaç doğrultusunda 16 Şubat 2011 tarihinde Kalkınma Bakanlığı tarafından e-Yazışma Projesi başlatılmıştır.

e-Yazışma Projesi, kurumlar arası elektronik ortamda resmi belge paylaşımı ya da iletimi yapılabilmesi için oluşturulmuş kurallar setini tanımlayan bir sistemdir. Bu sistem, belgelerin gönderici kurumda elektronik olarak oluşturulması ve alıcı kurumda açılarak kullanılmasına olanak sağlamaktadır. e-Yazışma Projesi, kurum içinde aktif şekilde kullanılan EBYS'lerin işleyişini etkilemeyen ve sisteme tamamlayıcı nitelikte bir çözüm getirerek, kurumlar arası resmi yazışmaların elektronik ortamda yapılmasını hedeflemektedir. e-Yazışma Projesi kapsamında kurumlar arasında iletilecek resmi yazıyı taşıyan pakete e-Yazışma Paketi (EYP) denir.

Kurumlar arası belge paylaşımında kullanılacak paketin elektronik ortamda sorunsuz bir şekilde aktarılması için ortak ve açık bir belge formatına ihtiyaç vardır. Bu ihtiyaçtan yola çıkılarak, EYP formatı uluslararası ve açık bir standart olan Açık Paketleme Yöntemleri (OPC) olarak belirlenmiştir. OPC, ZIP dosya yapısını temel alan geniş amaçlı bir dosya/bileşen paketleme aracıdır. OPC yapısı EYP'nin teknoloji ve platformdan bağımsız şekilde işlenmesine olanak sağlamaktadır.

EYP bileşenleri ve ilişkileri Şekil 4'de gösterilmektedir. EYP'yi oluşturan belgeye ilişkin zorunlu bileşenler üst yazı, üst veri, belge hedef ve elektronik imza; seçimli bileşenler ise ek, belge imza ve elektronik mühürdür.

Üst Yazı: Kamu kurum ve kuruluşlarındaki resmi yazıların ilgili mevzuatta belirtilen içerik, biçim ve görünümüyle saklanmasına olanak sağlayan elektronik dosyadır.

Üstveri: Bir belgenin oluşturulması, işlenmesi, iletilmesi ve saklanması sırasında ihtiyaç duyulan, belgeye ilişkin kimlik bilgileridir.

Belge Hedef: Paketin elektronik ortamda iletileceği alıcıların (kurum, kuruluş, tüzel veya gerçek kişi) bilgisinin listelendiği XML dosyasıdır.

Elektronik İmza: "Paket Özeti" bileşeninin kurum yetkilileri tarafından elektronik olarak imzalanmasıyla oluşan bileşendir.

Ek: Belgenin içeriğine ilişkin bilgi içeren ve "Üst Yazı" bileşeniyle ilişkilendirilmiş tüm elektronik dosyalardır.

Belge İmza: Üst yazıda bulunan tüm imzalara ilişkin künye bilgilerini barındıran XML dosyasıdır.

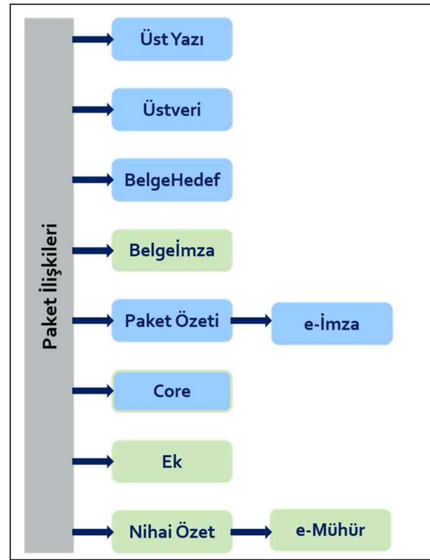
Elektronik Mühür: "Nihai Özet" bileşeninin kurum adına oluşturulan elektronik mühür sertifikası ile elektronik olarak imzalanmasıyla oluşan bileşendir.

EYP'yi oluşturan paket yapısına özel zorunlu bileşenler core ve paket özeti; seçimli bileşen ise nihai özettir.

Core: OPC tarafından tanımlanmış, pakete ait genel üstveri elemanlarını barındıran XML dosyasıdır.

Paket Özeti: "Üst Yazı", "Üstveri", "Belge Hedef" ve varsa "Ek" bileşenlerinin özet değerlerini içeren XML dosyasıdır.

Nihai Özet: "Üst Yazı", "Üstveri", "Belge Hedef", "Core", "Paket Özeti", "Elektronik İmza" ve varsa "Belge İmza" ile "Ek" bileşenlerinin özet değerlerini içeren XML dosyasıdır.



Şekil 4. e-Yazışma Paketi

e-Yazışma Paketi resmi yazıya ait bilgi ve bileşenlerin yanı sıra paketin kendisine ait tanımlayıcı bilgileri de içerir. Bileşenlerin adreslenmesi için OPC'de "ilişki" adıyla tanımlanan ve bileşenlerin paketle ve birbirleriyle ilişkilerini gösteren bir mekanizma kullanılmaktadır. Bu ilişkiler sayesinde, paketi işleyecek sistemler tüm paketi okumadan doğrudan ilgili bileşene ulaşabilir. Ayrıca, ileride pakete eklenmesi gereken bileşenler yeni ilişki türleri ile pakete eklenebilir (Rehber, 2016).

e-Yazışma Paketi içerisindeki belgelerin bütünlüğünün korunması ve kaynağının doğrulanmasına ek olarak hukuki geçerliliğinin sağlanması gerekmektedir. Bu gereklilikler elektronik imza kavramıyla karşılanmaktadır. EYP'de imzalanacak bileşenler, paket içerisinde belirli klasörlerde saklanır. Birden çok bileşeni tek bir

elektronik imzalama işlemi ile imzalamak amacıyla, "Paket Özeti" bileşeni imzalanır ve "Elektronik İmza" bileşeni olarak paket içerisine eklenir. Paket özeti, imzalanmak istenen her bir bileşenin paket içindeki yeri, paket dışındaki imzalanacak nesneler için nesneye ilişkin tanımlayıcı, imzaya dahil edilecek bileşenlerin matematiksel özet değerleri ve özet almakta kullanılan algoritma bilgisini içermektedir. e-Yazışma Projesi kapsamında oluşturulan elektronik imzaların, imza formatının Profil 4'e uygun olarak oluşturulması gerekmektedir.

e-Yazışma Projesi ve Elektronik Mühür

Gerçek ve tüzel kişilerin elektronik ortamda ayrımı kamunun önemli bir ihtiyacıdır. Günümüzde elektronik ortamda resmi bir yazının, kurumu temsil etmeye yetkisi olan kişi tarafından imzalanıp imzalanmadığı anlaşılamamaktadır. İmzacının kimliğini belirleyen sertifikaların yalnızca kişi adına üretilme zorunluluğu, sertifika içerisinde kurum adına imza yetkisi olduğuna dair bilgi bulunmaması bu problemin başlıca kaynağıdır. Bu durum kurumlar arası yazışmalarda ciddi sorunlar teşkil etmektedir. Bir kurum tarafından imzalanan yazının diğer kurum tarafından doğrulanması aşamasında, imzacı kurumun imzaya yetkili kişinin kimliğinin elektronik olmayan yollarla öğrenilmesi süreci yavaşlatmakta, bazen de güvenlik zafiyeti oluşturmaktadır. Bu soruna çözüm olarak kurum adına oluşturulan ve tüzel kişiyi temsil eden imza "elektronik mühür", imzalama işleminde kullanılan sertifika ise "elektronik (kurumsal) mühür sertifikası" olarak tanımlanmıştır. Kurumsal mühür sertifikalarının üretilebilmesi sayesinde, sertifikanın içerisinde kurum bilgisi bulunacak ve bu sayede elektronik doğrulama aşamasında güvenli ve hızlı biçimde yetki kontrolü yapılabilecektir.

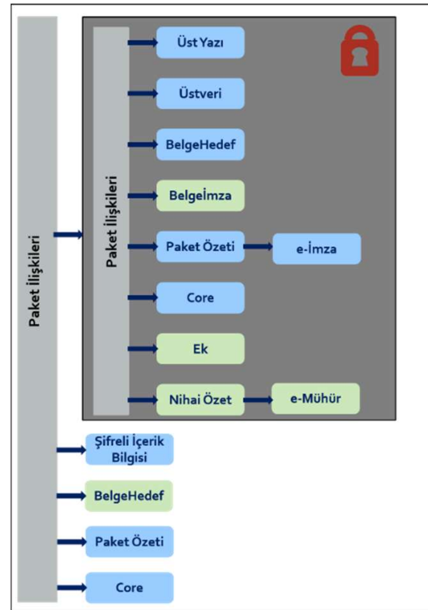
Elektronik imza ile elektronik mühür arasındaki en temel fark elektronik imzanın yalnızca gerçek kişiler için verilen NES ile elektronik mührünse yalnızca tüzel kişilere ait kimlik bilgilerini içeren Elektronik Mühür Sertifikası ile oluşturulmasıdır. Elektronik mühür sertifikaları, bu sertifikaları üretmeye yetkili kurum veya kuruluşlardan temin edilmelidir. Elektronik mührün amacı; imzalanan dokümanın kaynağının ve bütünlüğünün ispatlanmasıdır. Dokümanın kaynağı ile kastedilen, dokümanın ait olduğu kurum bilgisidir.

e-Yazışma Paketi'nde kullanılan elektronik mühür, e-Yazışma Paketi'ni oluşturan kurum veya kuruluşun kimliğinin doğrulanmasını sağlamaktadır. Elektronik imzalamaya benzer şekilde paket içerisinde bulunan bileşenlerin tek bir işlemle mühürlenmesi için "Nihai Özet" bileşeni mühürlenir ve "Elektronik Mühür" bileşeni olarak paket içerisine eklenir. "Nihai Özet", mühürlenmek istenen her bir bileşenin paket içindeki yeri, matematiksel özet değeri ve özet almakta kullanılan algoritma bilgisini içermektedir. e-Yazışma Projesi kapsamında oluşturulan elektronik mühürlerin, imza formatının Profil 4'e uygun olarak oluşturulması gerekmektedir.

E-Yazışma Projesi ve Şifreleme

E- yazışma projesinde şifrelemeye de imkan verilmektedir. Kurumlar arası iletilecek yazışma paketi şifreli olarak iletilebilmektedir. İlgili paket yapısında Şekil 5'de görüldüğü gibi; "Şifreli İçerik", "Şifreli İçerik Bilgisi", "Paket Özeti" ve "Core" bileşenlerini bulunmaktadır. Şifreli paketin içerisinde bulunan "Belge Hedef" bileşeni istenildiği durumda dış pakete de eklenebilmektedir. Eğer dış pakete eklenmezse şifre çözülmeden paketin hangi kurumlara iletileceği bilinememektedir.

Şifreleme işlemi CMS Envelope ile yapılmaktadır. CMS Envelope yapısında asimetrik kriptografi ve simetrik kriptografi birlikte kullanılmaktadır (RFC 5652, 2009). Öncelikle şifrelenecek olan veri, simetrik anahtarla şifrelenmektedir. Paketin gönderileceği kurumların şifreleme sertifikası Devlet Teşkilatı Merkezi Kayıt Sisteminden (DETSİS) çekilmekte ve her bir alıcı için ilgili simetrik anahtar, asimetrik kriptografi ile şifrelenerek CMS yapısına eklenmektedir. Dokümanın şifresini çözmek isteyen kurum kendi özel anahtarını kullanarak kendisi için şifrelenmiş veriyi çözmekte ve paketin şifrelendiği simetrik anahtarı elde etmektedir. Simetrik anahtarı kullanarak da paketin şifresini çözebilmektedir.



Şekil 5. Şifrelenmiş e-Yazışma Paketi

Kurum bir sebepten dolayı sertifikasını iptal edebilir veya sertifikasının süresi dolmuş olabilir. Bu sebeple ilgili paket kuruma şifreli olarak gönderilmeden önce kurumun sertifikasının geçerliliğine mutlaka bakılmalıdır.

İlgili sistem EYP'nin iletimi sırasında paket içeriğine üçüncü tarafların erişiminin engellenmesi amacıyla kurulmuştur. 2017/21 sayılı Başbakanlık Genelgesi ile kurumlara şifreleme anahtarları ve sertifikaları verme görevi Kamu SM'ye verilmiştir. Kamu SM tarafından üretilen anahtarlar kuruma teslim edilerek kurum tarafından saklanmakta ve üretilen anahtarların kopyası Kamu SM tarafından kesinlikle saklanmamaktadır. İlgili özel anahtarların kaybedilmesi durumunda söz konusu paketlerin şifresi çözülemez. Burada bütün sorumluluk kurumun üzerindedir. Bu sebeple e-Yazışma Teknik Rehberi'nde, şifreli olarak iletilen belgelerin kurumlara iletimi sağlandıktan sonra kurum bünyesinde şifresiz olarak saklanması gerektiği belirtilmektedir.

Kurumlar kendilerine gelen şifreli paketleri çözemediklerinde ya da şifre çözme işleminden sonra dış pakette bulunan "Paket Özeti" bileşeni ile imzalı olarak bulunan "Paket Özeti" bileşenini eşleştiremedikleri durumlarda ilgili paketi geçersiz olarak ele almalı ve kabul etmemelidir.

e-Yazışma Projesi kapsamında kullanılacak şifreleme bileşenleri e-Yazışma Teknik Rehberi'nde anlatılmakta ve şifreleme işlemleri için TÜBİTAK Kamu SM tarafından hazırlanan "Elektronik Belgeleri Açık Anahtar Altyapısı Kullanarak Güvenli İşleme Rehberi"ne atıfta bulunulmaktadır.

Uygulamalarda Dikkat Edilmesi Gereken Hususlar

Sistemdeki Güvenlik Katmanları bölümünde aktarıldığı üzere, e-Yazışma Paketi'nin kendine has bir takım bileşenleri bulunmaktadır. İmzalama, mühür ve şifreleme katmanlarının her biri e-Yazışma Paketi'nde var olan farklı bileşenler kullanılarak oluşturulur. EYP'nin bu kendine özgü bileşenlerini anlamak, imzalama, mühür ve şifreleme katmanlarını doğru bileşenler üzerine inşa etmek açısından oldukça önem teşkil etmektedir.

Uygulamaların EYP oluşturma modüllerinde, imza, mühür ve şifreleme katmanları oluşturulurken, katmanların hangi bileşenler kullanılarak oluşturulacağı, hangi bileşenlerin özet değerlerinin kullanılacağı ve elde edilen katmanların e-Yazışma Paketi'nin hangi bileşenleri içerisinde saklanacağı gibi bir takım konulara dikkat edilmesi gerekmektedir. Yanlış bileşenlerin ve özet değerlerinin kullanılması ya da elde edilen katmanların yanlış bileşenler içerisinde saklanması durumunda, düzgün bir e-Yazışma Paketi oluşturulamaz ve bu da e-Yazışma Paketi'nin doğrulanamaması anlamına gelir.

Uygulamaların EYP doğrulama modüllerinde ise, imza, mühür ve şifreleme katmanları doğrulanırken, imza oluşturma modülünde olduğu gibi kullanılacak bileşenlerin tespiti, katmanlardan elde edilen özet değerleri ile bileşenlerin özet değerlerinin karşılaştırılması gibi bir takım konulara dikkat edilmesi gerekmektedir. Katmanların üzerine inşa edildikleri bileşenlerden farklı bir bileşen kümesi alınarak doğrulama işlemi yapılmaya çalışılması, düzgün

oluşturulmuş bir e-Yazışma Paketi'nin doğrulanamamasıyla sonuçlanır. İmza doğrulama modüllerinde dikkat edilmesi gereken bir diğer husus ise, yanlış oluşturulmuş katmanlar içeren bir e-Yazışma Paketi'nin kesin olarak doğrulanmaması gerektiğidir. Bu da, e-Yazışma Paketi bileşenlerinin doğru bir şekilde anlaşılması ve katmanların üzerine inşa edildiği bileşenler haricindeki bileşenleri içermediğinin kontrol edilmesine bağlıdır.

İmzalama, mühür ve şifreleme güvenlik katmanları, Bölüm 3.1 ve Bölüm 3.2 olmak üzere iki alt bölümde incelenmektedir.

Bölüm 3.1'de yukarıda belirtilen konular göz önünde bulundurularak, uygulamaların EYP oluşturma modüllerinde imzalama, mühür ve şifreleme güvenlik katmanları oluşturulurken dikkat edilmesi gereken hususlar her bir güvenlik katmanına ayrılmış alt bölümlerde anlatılmaktadır.

Aynı şekilde, Bölüm 3.2'de, uygulamaların EYP doğrulama modüllerinde, bir e-Yazışma Paketi'nin imzalama, mühür ve şifreleme güvenlik katmanları doğrulanırken dikkat edilmesi gereken hususlar, her bir güvenlik katmanına ayrılmış alt bölümlerde anlatılmaktadır.

Uygulamaların EYP Oluşturma Modüllerinde Dikkat Edilmesi Gereken Hususlar

e-Yazışma Paketi'nin imzalama, mühür ve şifreleme katmanlarının oluşturulmasında dikkat edilmesi gereken hususlar her bir güvenlik katmanına özgü olarak aşağıdaki bölümlerde anlatılmaktadır.

İmza Katmanının Oluşturulmasında Dikkat Edilmesi Gereken Hususlar

e-Yazışma Paketi'nin imza katmanının oluşturulabilmesi için gerekli olan bileşenler Tablo 1'de belirtilmiştir. İlgili bileşenin paket içerisinde zorunlu olarak bulunması "Z" harfiyle, opsiyonel olarak bulunması ise "O" harfiyle ifade edilmektedir.

- Tablo 1'den anlaşılmaktadır ki, Üst Yazı, Üstveri, Paket Özeti ve Belge Hedef bileşenleri e-Yazışma Paketi imza katmanının oluşturulabilmesi için gereklidir. Uygulamaların EYP oluşturma modüllerinde, yukarıdaki tabloya uygun formatta imza katmanının oluşturulması gerekmektedir.
- Uygulamaların EYP oluşturma modüllerinde, e-Yazışma Paketi içerisine eklenecek olan bileşenlerin ekrandan kullanıcıya gösterilmesi ve e-Yazışma Paketi içerisine, yalnızca ekrandan gösterilen bileşenler eklenmesi gerekmektedir.
- e-Yazışma Paketi içerisine eklenmiş olan imzaya dahil olan bileşenlerin özet değerleri "Paket Özeti" bileşeni içerisinde yer almalıdır.
- "Üst Yazı" ve "Ek" bileşenlerindeki belgeler PDF/A formatında olmalıdır.

Bileşen Adı		
İmzaya Dâhil Olan İmza Özellikleri	Üst Yazı	Z
	Üstveri	Z
	Paket Özeti	Z
	Belge Hedef	Z
	Ek	O
	-DED	O
	-FZK	O
	-HRF	O
İmza	CAdES İmza	O
İmzaya Dâhil Olmayan İmza Özellikleri	Belge Imza	O
	Core	O
	Nihai Özet	O
	İmzasız Ekler	O

Tablo 1. EYP İçeriğindeki İmzaya Dahil Olan ve Olmayan Paket Bileşenleri

Mühür Katmanının Oluşturulmasında Dikkat Edilmesi Gereken Hususlar

- e-Yazışma Paketi'ne elektronik mührün konulmasının amacı, paketi oluşturan kurum veya kuruluşun kimliğinin doğrulanabilmesi olduğundan, elektronik mühür kurumun bilgilerini taşıyan mühür sertifikası ile oluşturulmalıdır.
- EYP oluşturma modüllerinde, mühür katmanı oluşturulurken Profil 4 imza kullanılmalıdır.
- Mühür katmanı, e-Yazışma Paketi "Nihai Özet" bileşeni imzalanarak oluşturulmalıdır.

Şifreleme Katmanının Oluşturulmasında Dikkat Edilmesi Gereken Hususlar

- Paketin şifrelenmesi için gerekli olan şifreleme sertifikası, uygulamaların EYP oluşturma modüllerinin DETSİS entegrasyonu aracılığıyla DETSİS web servisinden alınmalıdır.
- DETSİS web servisinden alınan sertifikalar doğrulanmalıdır.
- Şifrelenmiş bir paket "Şifreli İçerik Bilgisi", "Şifreli İçerik" ve "Paket Özeti" bileşenlerini içermelidir.
- Orijinal e-Yazışma Paketinin elektronik olarak şifrelenmiş hali "Şifreli İçerik" bileşeni içerisinde saklanmalıdır.
- "Şifreli İçerik Bilgisi" bileşeninde, e Yazışma Paketi'nin şifrelenmesi ve şifrenin açılması için gerekli olan bilgiler belirtilmelidir.

Uygulamaların EYP Doğrulama Modüllerinde Dikkat Edilmesi Gereken Hususlar

e-Yazışma Paketi'nin imza, mühür ve şifreleme katmanlarının doğrulanmasında dikkat edilmesi gereken hususlar her bir güvenlik katmanına özgü olarak aşağıdaki bölümlerde anlatılmaktadır.

İmza Katmanının Doğrulanmasında Dikkat Edilmesi Gereken Hususlar

- e-Yazışma Paketi'nin imza katmanının doğrulanmasında format kontrolü Tablo 1'e uygun olarak yapılmalıdır. Uygulamaların EYP doğrulama modüllerinde, tabloda zorunlu olarak belirtilen bileşenlerin paket içeriğinde var olduğu kontrol edilmelidir. Opsiyonel olarak belirtilen bileşenlerin paket içeriğinde bulunması zorunlu değildir. Ancak paket içeriğinde bulunan opsiyonel bileşenlerin de OPC görüntüleyici tarafından düzgün ayrıştırılarak görüntülenmesi gerekmektedir.
- EYP doğrulama modüllerinde, "Üstveri", "Üst Yazı" ve "BelgeHedef" bileşen özetlerinin "Paket Özeti" bileşeni içerisinde var olduğu ve bu bileşenlerin özet değerleriyle "Paket Özeti" bileşeni içerisinde belirtilen özet değerlerinin aynı olduğunun kontrol edilmesi gerekmektedir.
- e-Yazışma Paketi içerisinde var olan elektronik imza, "Paket Özeti" bileşeni imzalanarak oluşturulmalıdır. Uygulamaların EYP doğrulama modüllerinde, "Paket Özeti" bileşeni özet değeriyle elektronik imza içerisindeki özet değeri aynı olmalıdır.
- Uygulamaların EYP doğrulama modülleri ekranında, e-Yazışma Paketi içerisinde var olan bileşenlerin gösterilmesi gerekmektedir.

Mühür Katmanının Doğrulanmasında Dikkat Edilmesi Gereken Hususlar

- Uygulamaların EYP doğrulama modüllerinde "Nihai Özet" bileşeni içerisinde zorunlu olarak bulunması gereken bileşen özet değerlerinin varlığı ve doğruluğu kontrol edilmelidir.
- Elektronik mühür katmanının, "Nihai Özet" bileşeni kullanılarak oluşturulduğu kontrol edilmelidir.

Şifreleme Katmanının Doğrulanmasında Dikkat Edilmesi Gereken Hususlar

- Uygulamaların EYP doğrulama modüllerinde, şifreli bir paket içerisinde bulunan "Paket Özeti" bileşeni ile iç paketteki "Paket Özeti" bileşeninin aynı olduğu kontrol edilmelidir.

Sonuç

Kurumlar arası, elektronik ortamda yapılan resmi yazışmalarda kullanılacak ortak dil olması hedefiyle geliştirilen elektronik yazışma projesi, gerek sağladığı resmi

yazışmaya dair ihtiyaç duyulan ortak bileşenler gerekse verilerin güvenliğini sağlamak adına sunulan katmanlar sayesinde bu ihtiyacı karşılayacak çözüm olacağı düşünülmektedir. Projeyi kurumlarda hayata geçirecek ve bu proje dahilinde uygulamalar geliştirecek yazılım geliştiricilerin, bu çalışmada detaylandırılan güvenlik katmanlarını özümsemesi ve yine bu çalışmada yer verilen, geliştirme esnasında dikkat edilmesi gereken hususları göz önünde bulundurması, uygulamaların güvenli çalışması açısından çok önemlidir.

Bu özellikler göz önünde bulundurularak geliştirilen uygulamaların uluslararası standartlara uygunluğu 2017/21 Sayılı Başbakanlık Genelgesi'nde belirtildiği üzere TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi tarafından yapılmaktadır. Bu sebeple geliştiricilerin uygulamalarını canlı sistemlerde devreye almadan önce ilgili uyum değerlendirme hizmetini Kamu SM'den alması ve sonucunda verilecek olumlu rapor sonrası kullanmaya başlaması önemlidir. Bunun yanında Kamu SM, uyum değerlendirmeden olumlu sonuç alan uygulamaların bilgilerini kendi web sitesinde yayımlayacağından, uygulamalarını dışarıdan alan kurumların kendilerine verilen uygulama bilgilerini Kamu SM web sitesindeki bilgilerle kıyaslaması uygulamanın güvenliği açısından önem arz etmektedir.

Kaynakça

2017/21 Sayılı Başbakanlık Genelgesi (2017).

5070 sayılı Elektronik İmza Kanunu (2004).

Birlikte Çalışabilirlik Esasları Rehberi (2012). T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi.

Elektronik İmza Kullanım Profilleri Rehberi (2012). Bilgi Teknolojileri ve İletişim Kurumu.

ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES) (2013).

e-Yazışma Teknik Rehberi (2016). T.C. Kalkınma Bakanlığı.

ITU-T Recommendation X.509 (1997). Information Technology - Open Systems Interconnection - The Directory: Authentication Framework.

RFC 5652 - Cryptographic Message Syntax (CMS) (2009).

Estonya Siber Savaşı Örneğinde Enformasyon Yönetimi- Siber Güvenlik İlişkisini Sorgulamak

Tolga TELLAN

Ankara İl Sağlık Müdürlüğü

Öz

Çağımızda iletişim sürecindeki unsurlar adeta kontrol edilemeyecek düzeye ulaşmış ve bu unsurlar hakkında enformasyon sahibi olunması da bir zorunluluk haline gelmiştir. İstihbarat faaliyetlerinin temel amacını oluşturan bu zorunluluk, enformasyon kaynaklarına erişilmesi, kaynakların kategorileştirilmesi-ayrıştırılması-doğrulanması ve kesin bilgi haline dönüştürülmesi ile geçerlilik kazanmaktadır. Ekonomik, siyasal ve sosyal ilişkilerin değişen yapısı içinde enformasyona nasıl, nerede ve ne zaman erişilebileceği ile enformasyonun hangi süreçlerden geçerek bilgiye dönüştüğüne ilişkin arayışlar büyük önem taşımaya başlamıştır. Arayışlara koşut, sahip olunan bilginin epistemolojik gerçekliği (geçerliliği ve güvenilirliği) de sürekli tartışılır hale gelmiştir. Sıralanan gerekçeler ışığında, bu çalışmada istihbarat sürecinin günümüzde bir enformasyon yönetim ve kontrol stratejisi olarak düşünülmesinin gerekliliğine vurgu yapılmaktadır. Çalışma ile amaçlanan, 2007 Estonya Siber Savaşı örneğinden hareketle enformasyon yönetim stratejisinin siber güvenlik süreçlerine etkisini açığa çıkarmaktır. Sunulan amaç doğrultusunda konuyla ilgili literatür taramasını ve teorik tartışmaların sunumunu müteakiben vaka analizinden hareketle değerlendirmeler yapılmıştır. Uluslararası istihbarat faaliyetlerinin enformasyon yönetim sistemi olarak değerlendirilmesinin, terörizmle mücadelede kapsamlı bir strateji geliştirilebilmesi açısından büyük önem taşıdığı çalışmanın temel bulgusu olarak okunabilecektir.

Anahtar sözcükler: *Enformasyon Yönetimi, İstihbarat, Siber Savaş.*

Giriş

Bireylerin günlük yaşamlarının hemen her anı, çevrelerindeki varlıkları tanıma, onları anlamaya ve kavramaya çalışma, dış unsurların birbirleriyle olan ilişkilerini belirleme ve tüm öğrenilenleri kendi yaşamları için işler ve geçerli kılma uğraşıları ile doludur. Yaşamın enformasyonu oluşturma, elde etme ve dönüştürme uğraşısı olarak görülmesi, basit anlamıyla 'insan topluluklarının kurumsallaşması' olarak ifade edilen devletin de enformasyonu kendisi için varoluşsal bir çerçeveye yerleştirmesine neden olmaktadır. Devletler açısından enformasyonu yönetmek her şeyden önce toplama, ayrıştırma, birleştirme,

sınıflandırma, karşılaştırma, değerlendirme, analiz etme, karar verme ve yorumlama eylemlerinin bütünleşmiş bir halidir.

Tarihsel sürece bakıldığında, 1980'lerin sonu ile 1990'ların başında yaşanan olaylar XX. yüzyılda sonuçlanmamış ideolojik ve kültürel meselelerin biçim değiştirerek yeni döneme taşındığının açık bir göstergesi olmuştur. Küreselleşme eğilimi, çevre sorunları, farklı toplumsal grupların sosyal ya da hukuki talepleri enformasyon yığını ile boğuşulacak yeni bir dönemin haberini vermektedir. Dahası, bütün bu değişim ve dönüşüm talepleri, bir yandan global ölçekli bir kitleye televizyon ve internet aracılığıyla sunulurken, diğer yandan da iletişim kanalları Doğu Avrupa ya da Uzak Doğu Asya gibi farklı bölgelerde reformların önünü açacak kitlesel girişimleri ateşleyen unsur olarak anlam kazanmıştır (Taylor, 2003). Siyasetin uluslararasılaştığı ve sınır tanımaz özellikler kazandığı çalkantılı 1990'lar, 2000'lerin başından itibaren yerini –özellikle de 11 Eylül saldırıları sonrasında– uluslararası terörizmle mücadelenin yönlendiriciliğindeki yeni bir enformasyon sürecine bırakmıştır. Günümüz hükümetleri ister terörizm gibi ulusların ötesindeki tehditlerin yükselişi, ister küresel finansal kriz, iklim değişikliği ve şimdi de siber güvenlik olsun, sınırlarının ötesinde olanların çok daha önemli olduğu yeni nesil küresel sorunların çözümü gibi, sınırları içerisinde de olanları kontrol etmekte zorlanmaktadırlar (Singer ve Friedman, 2014). Artık devletler açısından, kritik enformasyona sahip olmak ile egemenliği korumak ve meşrulaştırmak eş anlamlı olarak kabul edilmektedir.

ABD Başkanı George Bush, 1990'ların başında 'Yeni Dünya Düzeni' (*New World Order*) kavramını ilk kez dile getirdiğinde bunun ne anlama geldiğine ilişkin detaylı bir bilgi bulunmamaktaydı. Bugün ise, 'Yeni Dünya Düzeni'nin, devletlerin karşı karşıya oldukları fırsat ve tehditleri görebilmek ve olaylara, kişilere, kurumlara, süreçlere ve eğilimlere ilişkin enformasyona sahip olabilmek için kesintisiz bir güç ve egemenlik mücadelesine girmeleri anlamına geldiği bilinmektedir. Enformasyona erişim mücadelesinin sonuçları, uluslararası arenadaki gücün birincil kaynağını belirginleştirmektedir. Ulus devletlerin, karar verme sürecinde kullandıkları enformasyonu kavrama ve bilgiye dönüştürmeye ilişkin eksiklikleri; hükümetlerin dış politikasında, şirketlerin global kaynak temininde ve bireylerin kültürlerarası iletişiminde yeni krizlere kapı aralamaktadır. Bu bağlamda, insan yaşamının güvenli kılınmasında birkaç temel faktörden hareketle çözümleme yapmaktan ziyade tüm enformasyonun sistematik olarak bütünleştirilmesinin ve analizinin gerekliliğine dikkat çeken yeni bir yaklaşım geliştirilmesi temel ihtiyaçtır. Konuya ilişkin temel öğeleri tartışmanın hedeflendiği bu çalışmada da, insan yaşamının güvenliğini ve yaşamın sürdürülebilirliğini tehdit eden terörize unsurların tespit edilmesi ile ilişkili olan açık istihbarat sürecinin, bir enformasyon yönetim ve kontrol stratejisi olarak düşünülmesinin gerekliliğine vurgu yapılması amaçlanmıştır.

Uluslararası istihbarat faaliyetlerinin enformasyon yönetim sisteminin parçası olarak değerlendirilmesi ve açık istihbarat konusundaki işbirliğinin enformasyon

yönetiminin global boyutu olarak kabul edilmesi, terörizmle mücadelede sosyal uzlaşıya varılmış bir stratejinin geliştirilebilmesi açısından büyük önem taşımaktadır. Konuya ilişkin tartışmalara giriş niteliğindeki bu çalışmada ilk olarak enformasyon yönetimi kavramı teorik olarak tartışılmakta, ikinci bölümde enformasyon yönetimi için bir stratejinin nasıl geliştirileceği sorgulanmakta, üçüncü bölümde enformasyon yönetimi ile istihbarat bağı siber güvenlik temelinde irdelenmekte, dördüncü bölümde Estonya'da 2007 yılında yaşanan ilk siber savaş vakasının analiz edilmesini müteakiben değerlendirmelerle sonuçlandırılmaktadır.

Enformasyon Yönetimi Kavramını Teorik Düzeyde Ele Almak

İnsan varlığının sürdürülmesinin gerekli ve zorunlu koşulu olarak açığa çıkan iletişim eylemi, özünde günlük yaşamımızla ilişkili, farklı maddi ve manevi yoğunluktaki içeriklere sahip verilere (*data*) ulaşma, onları anlamaya çalışma, karşılık beklemeksizin paylaşma, belli kıstaslar altında değiş-tokuş etme ya da sahiplenerek çevreye sunmaktan sakınma (gizil unsur olarak tutma) sürecidir. Herhangi bir birey için anlamsız, önemsiz, değersiz olarak algılanan veriler bir başka birey için yaşamsal öneme haiz, mutlaka ulaşılması gereken veri olarak görülebilmektedir. Bu farklılıklar genellikle saf\katışıksız (*pure*), basit, tekil ve yorumlanmamış (farklı anlamlandırmalarla ideolojik içerik kazanmamış) verilerin zaman ve mekân bağlamından kaynaklanmaktadır. Tarihin belli bir anında ya da dünya üzerindeki her hangi bir coğrafi mekânda kolay erişilebilir olan verinin başka bir zaman kesitinde ya da mekânsal konumda erişilemez olması durumu iletişim eyleminin biçimini\şeklini (*form of communication*) doğrudan belirlemektedir.

Zaman ve mekân bağlamındaki verilere erişim sonucunda, veriyi bilişsel ve psiko-kültürel süreçlerden geçirerek anlamlandırma, yani 'enformasyona dönüştürme' pratiği başlamaktadır. İnsan zihninin ham veriyi kendisi için anlamlı kılma çabaları sonucunda ortaya çıkan enformasyon (*information*), temelde oldukça kişisel, bireyin yorumlama çerçevesi doğrultusunda kodlanmış ve içinde yer alınan sosyal yaşam koşulları kapsamında diğer verilerle ilişkilendirilerek değer atfedilmiş bir içeriktir. Enformasyonun kişi için önemi, taşıdığı güvenilirlik ve geçerlilik ile doğru orantılıdır. Bireyin enformasyona erişim imkânlarının ölçümlenmesi, erişilen enformasyonun çarpıtılmış (*disinformation*) ya da uydurulmuş (*misinformation*) olup olmadığının denetlenmesi, enformasyon kaynaklarının bireyle ve birbirleriyle olan ilişkilerinin önem sırasına göre bağlantılandırılması ve derecelendirilmesi ile enformasyonun gelişim olanaklarının belirlenmesi, bahse konu güvenilirlik ile geçerliliğin yapısal uzantılarıdır. Enformasyonun ölçülebilir ve simgesel bir nitelik kazanması, iletişim eyleminin biçimine ve verinin enformasyona dönüşmesinde aktif bir rol oynayan bireyin sosyal güç ilişkilerindeki yerine bağlı olarak açığa çıkmaktadır. Enformasyon kavramı, özellikle Norbert Wiener'in II. Dünya Savaşı sonrası

geliştirdiği ‘sibernetik’ kavramı ile Claude Shannon ve Warren Weaver tarafından 1949 yılında geliştirilen ‘matematiksel iletişim modeli’ çerçevesinde yeniden anlamlandırılmıştır. Wiener’e göre “enformasyon, evrenin fiilen duraklamasına neden olacak entropik dürtüye karşı hayatın gerçekleştirdiği karşı saldırıların esas parçasından başka bir şey değildir” (Kumar, 2004) İletişimin düz ve çizgisel bir süreç olarak betimlendiği matematiksel iletişim modelinde ise ‘kaynaktan hedefe’ doğru mesaj aktarımı esastır: “Süreç içinde en başta iletilecek gönderi veya gönderiler zincirini üreten enformasyon kaynağı gelir. İkinci olarak gönderi, iletici tarafından sinyallere dönüştürülür. Sinyaller alıcıya yönelen kanala uygun hale getirilmelidir. Alıcının işlevi ileticinin tam tersidir. Alıcı sinyali gönderi olarak tekrardan oluşturur. Alınan gönderi daha sonra hedefe ulaşır. Sinyal gürültüden etkilenebilir, örneğin aynı anda aynı kanalda birçok sinyalin olması halinde engelleme meydana gelebilir. Sonuçta, iletilen ile alınan sinyal farklı olabilir” (McQuail ve Windahl, 1997). Bu tanımlamalar çerçevesinde enformasyon kavramının betimlenmesinde olgunun teknolojik yönü ile ‘veri-data-byte’ gibi adlandırmalarla ölçülebilirliğe ve nesnelliğe vurgu yapılmaya başlamıştır. Ancak ölçülebilirliğe yönelme, enformasyonun, anlam, nitelik ve ticari olarak kavranabilirliğini daraltmakta; ‘bilgi’den felsefi olarak farklılaşmasını imkânsızlaştırmaktadır (Törenli, 2004). Bu bağlamda, Marc Porat’ın “enformasyon örgütlenmiş ve iletilen veridir” (Porat, 1977’den aktaran Castells, 2005) tanımı, halen geçerliliğini koruyan bir betimleme olarak karşımızda durmaktadır.

Enformasyonun somutluk kazanmasıyla birlikte, sahipliği, erişilebilirliği, erişim tekniklerinin kısıtlılığı ile erişim kanallarının sınırlılığı gibi unsurlar gündeme gelmektedir. Enformasyonun mülkiyetine yönelik bu soruların yanıtı, aynı zamanda ‘neyin bilgi olduğu’ konusunu da tartışmaya açmaktadır. Bilgi (*knowledge*), en genel –ve verimsiz ifadesiyle– ‘metalaşmış enformasyondur’. Bilgiyi enformasyonun ötesine taşıyan esas öğe, yeni bir örgütlenme dizgesi içinde bulunması ve bu örgütlenme dizgesinin çerçevesinin de sahiplik ilişkileri ile sınırlandırılmış olmasıdır. Bilgi, mantık süzgecinden geçerek ispat edilebilen yargılardan ya da deneysel gözlemlerle belli koşullar altında sonuçları gösterilen olgulardan müteşekkil enformasyonu, diğerlerine iletme sürecinin açığa çıkardığı ve sahipliği ile erişim için katlanılacak bedelinin bilindiği ifadeler bütünüdür. Bilgi de, enformasyonun kişisel yorumlama ve değer atfetme sürecinin ötesinde; sosyal gerçekler olarak kabullere ve belli koşullar altında sahip olmanın gücüne odaklanılmaktadır. Hangi enformasyonun, ne zaman, nerede, nasıl ve kimlerce bilgiye dönüştürüleceği ile bilgi olarak anlam kazananın neden sınırlı bir sosyal grubun –ki bu grup toplumsal elitler, zenginler, akademisyenler ya da bürokratlar olabileceği gibi alt gruplar, egemen düzen karşıtları, etnik azınlıklar ya da dar bir sosyo-kültürel kesittekiler de olabilmektedir– kontrolünde olduğu soruları, dikkatleri enformasyonun bilgiye dönüşümündeki ‘şeyleşmeye’ yöneltmektedir. Bu ‘şeyleşme’, enformasyonun metalaşması, ticarileşmesi ve bedeli ödenmek koşuluyla paylaşılarak toplumsallaşması süreci şeklinde günlük yaşamda anlam bulmaktadır:

> "Bilgi bir depolama olmaktan çok, bir işlemdir. Bilgisi ve bilimsel durumu o günkü gereksinimi karşılayacak durumda olan, sürekli bir şekilde dış dünyayı gözlemleme işleminde bilginin önemini kavrayan ve davranışlarını bu gerçeğin ışığında etkin bir şekilde düzenleyebilen ülkeler, en büyük güvenlik içindedir. Başka bir deyişle, büyük bir dikkatle kitaplara aktarılıp üstüne gizlilik damgası vurularak, kitaplıklarda saklanan hiçbir bilimsel araştırma, bilgi düzeyi sürekli olarak, etkin bir şekilde yükselen bir dünya içinde bizi kısa bir süre için bile korumaya yeterli değildir" (Wiener, 1975).

Uluslararası güvenlik politikalarının yeni görünümüyle bağlantılı olarak enformasyon, analistlerin üzerinde değerlendirmede bulunacakları materyalin bütününe işaret etmektedir. Farklı süreçlerden geçerek işlenen, belirli kurallar çerçevesinde yeniden düzenlenen, diğer anlamlı verilerle ilişkilendirilen, bilişsel kaynaklara başvurularak anlam katılan ve en önemlisi de hedefte 'fark yaratan'/yeni etkilere zemin hazırlayan istihbarat yoğun enformasyon, güvenlik stratejisi kapsamındaki sonuçları ortaya konulduğu ya da sahiplenildiği andan itibaren 'bilgi' olarak adlandırılmaktadır. Ulusal-uluslararası güvenlik bağlamında bilgi, genellikle gizli tutulan, sahip olan taraf için potansiyel güç açığa çıkaran bir unsurdur. Çok farklı alanlarda uzmanlaşmış analistlerin üzerinde uzlaştıkları husus ise, bilginin nicelikten öte nitelikli enformasyon birikimine dayalı olmasıdır. Elbette elde edilecek olan her ayrıntı, enformasyonun anlamlandırılması ve ilişkilendirilmesi bağlamında aydınlatıcı olabilmektedir; niceliksel olarak fazla olan ancak gerçeklikle örtüşmeyen enformasyonun, verilecek kararların sağlıklı ve başarılı sonuçlar doğurmasını engelleyici nitelikte olacağı da göz önünde bulundurulmalıdır:

> "Uzman bir analistin, enformasyona dayalı bir hükme varabilmesine yetecek düzeyde minimum enformasyona ulaşmasının ardından, elde edilecek olan ilave enformasyon genellikle tahminlerinin doğruluğunu artırıcı bir nitelik taşımamaktadır. Bununla beraber, ilave enformasyon, kendine fazla güvenme derecesine değin uzanan bir tarzda, analizi yapanın kararından daha da fazla emin olmasını sağlamaktadır" (Hever Jr., 1999).

Uluslararası güvenlik politikasında, verilerin kullanılabilirliği zamansal kısıtlara, enformasyonun etkililiği bütüncül erişim ve yorumlama becerisine, bilginin bağlamı da sahip olunanın gücüne bağlı olarak konjonktürel ve stratejiktir. Bu çerçevede, terörizmle mücadele amaçlı yeni bir uluslararası güvenlik zemini oluşturmanın ilk koşulu, sınırsız miktardaki enformasyon ile sosyal değişkenler arasındaki ilişkileri kurgulayarak, analizler yapmaktır. Bu koşulun sağlanmasını takiben istihbarat analizlerinin uygulanırlığının, enformasyon yönetimi süreci kapsamında sürekli gelişim gösteren bir kurumsallaşma içerisinde olduğunun vurgulanması gerekmektedir.

Enformasyon Yönetimi Stratejisi Geliştirmek

İnsanlık tarihinin hemen her döneminde kritik öneme sahip olan enformatif içerik, sosyal grupların, cemiyetlerin, devletlerin ve hatta uluslararası örgütlerin gelişiminde büyük bir önem arz etmiş ve güç siyasetinin temel aktörlerinden biri olarak anlam kazanmıştır. Günümüzde de uluslararası ilişkilerin ve gün geçtikçe

benzeşmekte olan ekonomik, siyasal ve kültürel işleyiş tarzlarının altyapısını oluşturan 'enformasyon', olayların nedenlerinin ortaya konulması, farklı düşünce, inanç ve davranışların tarihsel köklerinin irdelenerek değerlendirilmesi ile basitten karmaşığa değin çeşitlenen ve kapsam olarak genişleyen iletişim süreçlerinin anlamlandırılabilmesi açısından temel unsur olarak karşımıza çıkmaktadır.

Enformasyon iletimi sonrasında oluşan gündem ise farklı içerik yoğunlukları, örtüşen ya da çatışan politikalar ile enformasyona erişen\erişemeyen aktörler tarafından belirlenmektedir. Ancak gündemin belirlenebilmesi için, enformasyona sahip olanların enformasyonu güç siyasasının unsuru olarak algılayabilmeleri ve enformasyonu kullanabilme becerisine sahip olmaları gerekmektedir. Modern siyasal yaşamda güçler hiyerarşisi bir piramit olarak karakterize edilmektedir. "Sadece piramidin en üstünde bulunanlar konulara/stratejilere/ planlara tamamen hakim olmaktadırlar. Piramidin daha alt seviyelerinde bulunanlar ise salt işlerini yürütebilecek seviyedeki enformasyondan haberdar olabilmektedirler" (Knight-Jadczyk ve Quinn, 2006). Enformasyonun tamamından, bağlamından ya da mekânsal-zamansal kısıtlarından haberdar olmamak; enformasyona erişimde sorunlar yaşamak ve enformasyonu bilgiye dönüştürememek, özellikle kaotik ve çatışmacı iletişimin egemen olduğu koşullarda daha önemli sorunlara neden olmaktadır.

Ulusal ya da uluslararası güvenlik amaçlı istihbarat faaliyetleri sırasında, enformasyona erişim gediklerinin minimum düzeye indirgenmesi ve tüm kanallardan yararlanılmaya çalışılması, terörist girişimleri engelleyecek bilginin açığa çıkarılabilmesinde büyük önem taşımaktadır. Enformasyonun hangi kanallardan (kimden), hangi yöntemlerle (nasıl) ve hangi koşullarda (nerede ve ne zaman) elde edilebileceğinin; hangi tekniklerle kontrol edilerek doğrulanabileceğinin (güvenilirliğinin ve geçerliliğinin sınanabileceğinin) ve güvenlik politikasının parçası olacak bir bilgiye ne türden işlemlerle dönüştürülebileceğinin başlangıç aşamasından itibaren belirlenmiş olması gerekmektedir (Hever Jr., 1999). Bu bağlamda, operasyonel istihbarat ile açık istihbaratın enformasyon yönetim stratejisi de farklılaşmaktadır. Operasyonel istihbarat sürecinde enformasyon yönetimi çabukluk, öznel iletişim becerisi ve saha deneyimi gerektirirken; açık istihbarat sürecinde enformasyon yönetimi neyin önemli nelerin de önemsiz olduğunu ayırt edebilme, enformasyonu analiz ederek bilgiye dönüştürebilme ve çarpıtılmış ya da uydurulmuş enformasyondaki amaçlılığı dahi ortaya çıkarabilecek birikime sahip olma yeteneklerinin kullanılmasını gerektirmektedir. Ancak nihai noktada her iki kanaldan toplanan enformasyon bir konuya ilişkin bilginin parçaları olarak ifade edilebilecektir. Örneğin 11 Eylül 2001 saldırıları sonrasında, uluslararası yolculuklarda güvenlik prosedürlerinin daha da karmaşıklaşmasının, biyometrik kimlik kartları ile çipli pasaport kullanımına yönelinmesinin, ulusal ve uluslararası güvenlik kuruluşlarının haberleşmede sayısal ağ ve internet hizmetlerine daha yoğun

biçimde başvurmalarının ve terör eylemcilerinin psikolojileri ile davranışlarını anlamaya yardımcı olacak akademik araştırmalar yürütülmesinin; terörist gruplara yönelik takip, dinleme, içeriden enformasyon sızdırma ya da grubun içine istihbaratçı personel yerleştirme sürecinden amaçsal olarak farksız olduğu görülmektedir. Her iki istihbarat sürecinin de ortak noktası, ticari uçakları kullanarak sivil halka yönelik yeni saldırıların gerçekleştirilmesinin önüne geçecek bilgiye en kısa sürede ve en düşük maliyetle ulaşmaktır.

Enformasyonun yorumlanma süreci, etkin bir sonuca ulaşabilmek için çok sayıda analitik prosedürün takip edilmesine ve yönetsel sorumluluğun üstlenilmesine bağlıdır. İstihbarat sürecinde kaynakların, analiz aşamasının incelikleri hakkında bilgi sahibi olmaları, veri toplanmasında hassasiyet gösterilmesini sağlamaktadır. Veri toplama aşamasında belirli kriterlerin gözetilmemesi, analizlerin sonuçlarını da doğrudan etkileyecektir. Mevcut durum ile ilerde yaşanması muhtemel gelişmeler hakkında bir karara varılabilmesi için önemli bileşenlerin bir arada değerlendirilmesine gereksinim vardır (Hever Jr., 1999). Enformasyon kontrol ve yönetim birimlerinde eşzamanlı olarak tüm veriler tanımlanmakta, sınıflandırılmakta ve uygun ölçüm tekniklerinin belirlenmesi sonucunda anlamlandırılarak doğruluk, geçerlilik ve güvenilirlik bakımından test edilmektedir. Analizin bütününde, enformasyonun elde edilme yöntemi en önemli aşamayı oluşturmaktadır. Çarpıtılmış, uydurulmuş ya da eksik enformasyon ile yapılan analizler geçerli ilişkiselliklerin kurulmasını engellediği gibi alınacak stratejik kararlarda da yanlışlıklara neden olmaktadır.

Analitik sürecin anlaşılabilmesi, mozaik metafor stratejisi ile değişime uğramıştır. İstihbaratta mozaik metafor stratejisine göre küçük enformasyon parçaları, adeta bir mozaik döşenir ya da yapboz bulmacası çözer gibi 'gerçekliğin açık bir resminin ortaya konulabilmesi' bağlamında toplanmakta ve birleştirilmektedir. Küçük enformasyon parçalarının, bütün resmin basit materyalleri olmaları nedeniyle, toplanmaları ve biriktirilmeleri çok önemlidir; analistler açısından en küçük bir veri bile yapboz üzerindeki parçayı tamamlamada yararlı olacaktır. Günümüzün geniş, teknik istihbarat toplama sistemleri mozaik metafor stratejisi esasında işlemektedir. Ancak, bilişsel psikoloji, istihbarat uzmanlarının bu şekilde çalışmadıklarını ileri sürmektedir. Analistler genellikle çok sayıda, farklı resimlere uyacak parçalara yönelmektedirler. Analistler, tüm parçaların bir araya gelmesi ile ulaşılacak olan resim yerine, tipik olarak zihinlerinde bir resim biçimlendirmekte ve bu resme uyacak enformasyon parçacıklarını seçmektedirler. Bu durum da, istihbarat için geliştirilen enformasyon yönetimi stratejisi ile enformasyon yönetimine dayalı güvenlik politikası uygulamalarının birbirinden farklılaşmasına ve ayrıksılaşmasına neden olmaktadır.

Enformasyon Yönetimi-İstihbarat Bağı

Temel anlamıyla istihbarat, devletlerin, kurumların, uluslararası güvenlik kuruluşlarının ve hatta günümüzde şirketler ile bireylerin enformasyonun

işlenmesi, kodlanması ve kıymetlendirilmesi sonucunda üretilen bilgiye belirli koşullar altında erişme becerisidir. Güvenlik bağlamındaki istihbarat ise, devletlerin ve yurttaşlarının varlıklarını maddi veya manevi bakımdan tehlikeye düşürecek herhangi bir durum ya da olay karşısında, karar mekanizmasının etkin ve etkileşimsel bağlamda sorunsuz işleyebilmesi için, anlık ya da planlı olarak yürütülen, kısa ve uzun vadeli olumsuz sonuçlar doğuracak tüm ilişki ve işbirliklerini soruşturan, olası güvenlik tehditlerine karşı tedbirli olabilmek açısından her türlü içeriği ve tekniği kullanan, elde edildiği andan itibaren sahibine üstünlük kazandıran enformasyon derleme ve dönüştürme sürecidir. Tehdit unsuru oluşturan birey veya bireyler topluluğunun -ulusal ya da uluslararası çapta olabilir- uzun vadede neler planladığı, hangi kişi veya kurumlarla işbirliği yaptığı, yasal olan ve olmayan ilişkilerinin ve eylemlerinin neler olduğu konusunda enformasyon toplamak kapsamlı inceleme, analiz ve doğrulama süreci gerektirmektedir. İstihbarat, temelde enformasyon 'elde etme' sürecine işaret ederken; elde edilen enformasyonu kullanan ya da stratejik olarak 'doğru' ve 'etkili' olacağı zamanda kullanma potansiyeli taşıyan kişiler, kurumlar ya da hükümetler dünya ekonomik, politik ve askeri arenasında kilit konuma gelmektedirler.

Hızlı bir dönüşüm yaşayan dünya siyasetinde ulusların karşı karşıya oldukları tehditler nicelik olarak artmakta; nitelik olarak da çeşitlenmektedir. Global ekonomik yapı, enformasyonun dolaşımını hızlandırmakta ve derinleşmektedir. Bu bağlamda 'gerçek', 'doğru' ve 'gerekli' enformasyonun zamanında elde edilmesi ile karar mekanizmaları tarafından işleme konulması hayati önem kazanmaktadır. "İstihbaratın analizine ilişkin olarak karşılaşılan sorunların temelinde, ulaşılabilen enformasyonun yetersiz olması yer almaktadır" (Hever Jr., 1999). Enformasyon yönetimine ilişkin güncel stratejiler, analitik araştırmaların artırılmasına, analitik metotların geliştirilmesine ya da analitik hükme varılmasını ve kararlar alınmasını sağlayacak sosyo-psikolojik araştırmaların çoğalmasına vurgu yapmakla birlikte, ülkelerin bütçe ödeneklerinden enformasyon yönetimine ayrılan payların sabit kaldığı veya azaldığı gözlemlenmektedir. Güvenlik sorunlarının çoğalması ve uluslararası terörizmin ekonomik, siyasi ve askeri yeni dalgası ile mücadelenin gün geçtikçe zorlaşmasına karşın, enformasyon yönetimine ayrılan finansal kaynakların kısıtlı düzeyde kalması şaşırtıcıdır. Hükümetler, kurumlar, şirketler ve bireyler 'maliyetsiz bilgiye sınırsız erişim' talepleriyle, enformasyon yönetimi için bir strateji geliştirmemekte ya da geliştirdikleri stratejinin adeta 'sıfır maliyet' politikasına odaklanmasını istemektedirler. Ancak açık istihbaratın yürütülebilmesi ve internet aracılığıyla gerçekleşen veri akışının kontrol edilebilmesi için dahi sabit ve değişken maliyetlere katlanılması gerekmektedir.

Tarihsel sürece bakıldığında, son yüzyıllık dönemde dünya haritasındaki sınırların konjonktüre, jeopolitik faktörlere ve askeri-siyasi-ideolojik mücadelelere bağlı olarak değiştiği, bir gerçeklik olarak karşımıza çıkmaktadır.

Ulus devlet olmak, sadece ülke içi ilişkileri yürütmek, toplumsal düzeni, refahı ve barışı sağlamak anlamına gelmemektedir. Her ülke üretim gücü, ekonomik kaynakları, jeopolitik konumu, sınır komşuları ve ülkelerle kurduğu ilişkiler kapsamında –ki burada sadece ülkelerin kendi aralarındaki ilişkileri değil bir bütün olarak ülkenin uluslararası ilişki tarzı önem kazanmaktadır– varlığını sürdürebilmek ve yurttaşlarının haklarını koruyabilmek için uluslararası ilişkilerini düzenlemek zorundadır. Ülkeler arasındaki ilişkiler, tarihi ve konjonktürel güç konumundaki ülkeler, uluslararası örgütler ile ekonomik-askeri ortaklıklar tarafından yönlendirilmekteyse de politik arenada hiçbir zaman dillendirilmeyen amaç ve hedefler doğrultusunda her an açmazlarla karşılaşılabilmekte ve bu durum, çok katı askeri-siyasi-ekonomik çözüm yolları geliştirilmesini gerekli kılabilmektedir. Bu çerçevede, uluslararası ilişkilerde 'enformasyonun propaganda amaçlı kullanımı' yöntemini kullanan güçlerin eylemlerine meşruiyet kazandırma çabası içinde oldukları bilinen bir durumdur. Tarihte uluslararası dengelerin kurulması ve güç kullanımının çeşitli örneklerine rastlamak mümkündür. Bu bağlamda iletişim kanallarının ve medya mensuplarının desteğine başvurulması, uygulamaların meşruiyet kazanması bağlamında büyük öneme sahiptir. Özellikle Cezayir, Vietnam, Afganistan gibi ülkelere yapılan dış müdahalelerde izlenen iletişim politikaları ile Körfez Savaşı'nın medyatikleştirilmesi bu siyasetin açık göstergeleridir. Körfez Savaşı'nda aralarında General Norman Schwarzkopf'un da yer aldığı çok sayıda kıdemli ABD'li komutanın Vietnam deneyimini yaşamış olması, savaş boyunca nasıl bir iletişim stratejisi izleneceği ve geçmişte yapılan hataların tekrarlanmaması için neler yapılacağı noktasında karar verilmesini kolaylaştırmıştır. Körfez Savaşı'nın stratejisi, açık ve gerçekleştirilebilir askeri hedeflerin belirlenmesi, Washington'un siyasi müdahalesinin minimum düzeyde tutulması, beklenmeyen durumların ortaya çıkma ihtimalinin asgari düzeye çekilmesi anlamında savaşın kısa sürede tamamlanması ve uluslararası medya yayınları yoluyla kamuoyu desteği sağlanması ilkelerine dayanmaktaydı. Farklı ülkelerden gelen ve sayıları 1500'ü aşan uluslararası muhabir topluluğu, en yeni teknolojik donanımla –taşınabilir uydu antenleri, portatif telefonlar ve muhabirlerin kendi ofislerine veri akışı sağlayabilmeleri amacıyla, resmi iletişim kanallarını geri plana itme yeteneği olan internet bağlantılı dizüstü bilgisayarlar–, bölgeye akın etmiştir. Bu bağlamda kitle iletişim araçları, bir propaganda savaşının temel kanalı haline gelmiştir. Bağdat yönetimi hava bombardımanının başlamasıyla birlikte koalisyon ülkelerinden muhabirlerin ateş altındaki Irak'tan yayın yapmalarına izin vermiştir. Saddam Hüseyin yönetimi, muhabirlerin Irak'ın başkentinden yayın yapmaları sonucunda Batılı izleyicilerin 'mide bulandırıcı' savaş görüntüleri ile savaşın bitirilmesi yönünde bir karşıtlık içerisine gireceklerini tahmin ettiğinden medyaya görece destek sağlamıştır. Tüm bu yaşananlar göstermiştir ki, medya artık çatışmanın sadece basit bir gözlemcisi olmayıp, doğrudan ön cephesinde yer almaktadır. Bu durum ABD'nin 2001'de başlattığı Afganistan harekatı ile 2003-2010 dönemindeki Irak Savaşı'nın 'yeni çağın medya savaşları' olarak adlandırılmasını da kolaylaştırmıştır. Yaşanan dönüşüm, 'savaş alanında askeri birimlere iliştirilen küçük gruplar halindeki

muhabir havuzları'nın oluşturulmasına dayalı yeni bir haberci sevk ve idare rejimi (*embedded journalism*) geliştirilmesini de sağlamıştır. Körfez Savaşı döneminde, muhabirlerin çeşitli ihtiyaçlarının tedarikini sağlamak üzere Ortak Enformasyon Bürosu (*Joint Information Bureau–JIB*) kurulması medya-askeri güç ittifakını belirginleştirmektedir. Uydu haberleşme sistemlerinin, bilgisayar ağlarının ve yeni iletişim teknolojilerinin kullanımı ve CNN'in 24 saat canlı yayını aracılığıyla ilk gerçek zamanlı askeri harekat sunumu yapması nedeniyle 1990-1991 Körfez Savaşı, 'ilk enformasyon savaşı' olarak adlandırılmıştır. Bu yeni düşünme tarzını tanımlamak için 'siber savaş' (*cyberwar*), 'bilgisayar ağı esaslı saldırı ve savunma' (*computer network attack and defense*), 'elektronik savaş' (*electronic warfare*), 'enfo-bomba' (*info-bombs*) ve 'enfo-savaşçılar' (*info-warriors*) gibi kavramların kullanıldığı bütünüyle yeni bir terminoloji geliştirilmiştir (Taylor, 2003).

Başlangıcından itibaren istihbarat faaliyetlerinde enformasyon elde etme ve yönetme sürecinin temel yöntemi 'gizlilik' olmuşsa da; günümüz dünyasında ilişkilerin çeşitlenmesi ve karmaşıklaşması nedeniyle 'açık kaynak'lar da etkin olarak kullanılmaya başlanmıştır. Güvenlik amaçlı istihbarat faaliyetlerinde farklı tekniklerin yanı sıra 'insan kaynakları yönetimi' ile 'açık kaynak kullanımı' yaygınlık kazanmıştır. İstihbarat elemanlarının, insan kaynaklı enformasyon toplamaya çalışması, bire bir kaynaklara erişimi mümkün kılmakla birlikte dolaylı risk ve sorunları da beraberinde getirmektedir. Buna karşın uluslararası terörizmin ağ temelli, çokuluslu ve kendi finansal ilişkilerini oluşturan yeni örgütlenmesi, açık kaynak kullanımına duyulan gereksinimi artırmış; çok yönlü eğitim görmüş, genel kültür yönünden zengin dağarcığı bulunan, tarih bilgisine sahip, birkaç dil bilen, analitik düşünebilen, elde edilen verileri ilişkilendirebilen-ayrıştırabilen-aşamalandırabilen, insan psikolojisinden anlayan, pratik zekaya sahip, anlık önlemler ve çözüm önerileri geliştirebilen açık kaynak analistlerine duyulan ihtiyaç belirginlik kazanmıştır. Günümüzde enformasyonun büyük bir kısmının açık kaynaklardan ediniliyor olması, istihbaratın gizli ve operasyonel yönünün mutlak suretle açık kaynaklardan elde edilecek enformatif birikimin üzerine inşa edilmesi gerektiğini ortaya koymaktadır.

Vaka İncelemesi: İlk Siber Savaştan 10 Yıl Sonra

1.312.000 yerleşik nüfusu ve 2016 sonu itibariyle 23.1 milyar ABD Dolarlık GSMH'si ile Avrupa'nın görece küçük ancak efektif ekonomilerinden biri olan Estonya, bilişim alanına yüksek düzeyde yatırım yapmış bir Baltık cumhuriyetidir. I. Dünya Savaşı sonrası Rusya ile siyasi gerginlik ve askeri çatışma yaşayan Estonya'nın SSCB'ye katılma süreci II. Dünya Savaşı sonrasındaki Bloklaşma döneminde olmuştur. Baltık bölgesine biçilen ekonomik rol içerisinde üretime özerk federal bölge olarak dahil olan ülke, parçalanma sürecinin başlamasıyla 20 Ağustos 1991 itibariyle bağımsızlığını ilan etmiş; 2004 yılında ise AB'ye katılmış ve NATO üyesi olmuştur.

Estonya genelindeki Rus karşıtı eğilimler 2007 yılında yaşanan Bronz Asker Anıtı olaylarıyla zirveye çıkmıştır. II. Dünya Savaşı sırasında Nazi işgaline karşı savaşıp ölen Sovyet askerlerini temsil eden 'Tallinn'in Kurtarıcısı Anıtı'nın Başkent Tallinn'in merkezinden bir askeri mezarlığa nakledilmesiyle açığa çıkan gerginlik, bilinen ilk siber savaşın da başlatıcısı olmuştur. Estonyalı milliyetçilerce Sovyet işgalinin sembolü olarak görülen anıtın yerinin değiştirilmesiyle birlikte Rus hackerlarca, Estonya kamu kurumlarının, bankalarının, siyasal partilerinin ve medya kuruluşlarının web sitelerine yönelik DoS ve DDos saldırıları gerçekleştirilmiştir. "Estonya Dışişleri Bakanı Urmas Paet, Kremlin'i saldırıda doğrudan dahli olmakla suçladı. Sonunda Kremlin destekli yurtsever gençlik grubu 'Nashi' (Bizimkiler) DoS saldırılarının sorumluluğunu üstlendi" (Ross, 2017).

Estonya'nın bilişim dünyasındaki konumu ise farklı bir düzleme oturtulmalıdır. 2014 yılı itibariyle nüfusunun % 82'sinin internet kullanıcısı (15 yaş üzeri nüfusun cep telefonu penetrasyon oranı ise % 100) olduğu, ülke coğrafyasının 1140 farklı noktasında vatandaşlar için ücretsiz wi-fi uygulamasının sunulduğu, vergi beyannamesi düzenlenmesinden şirket kurulmasına -hatta seçimlerde oy kullanmaya değin- hemen her türlü işlemin siber ortamda yapıldığı, sağlık sistemi kayıtlarının bütünüyle elektronik ortama taşındığı, ilkokuldan itibaren öğrencilere programlama ve kodlamanın öğretildiği ülkede; 2017 yılı itibariyle ödeme hareketlerinin sanal para 'estcoint' ile yapılması yönünde ilk adımlar atılmış ve anayasada "internet, ücretsiz karşılanması gereken bir vatandaşlık hakkıdır" hükmüne yer verilmiştir. 2001 yılında uygulamaya sokulan dijital otoban *X-Road* ile ülke genelinde tüm yazılımların tek bir platforma entegre edilmesi hedeflenmektedir. Kamunun siber dünyaya açılmasıyla verimlilik, tasarruf ve şeffaflık konularında gelişim gösterilmesi beklenmekte olup, bu kapsamda vergi ve gümrük işlemlerinin % 94'ü, bankacılık işlemlerinin ise % 97'si internet üzerinden gerçekleştirilir hale gelmiştir (Bıçakçı, 2013; BBC, 2016; NTV, 2017).

Anıtın mezarlığa nakledilmesine karşı çıkan Rus kökenli Estonya vatandaşlarının -ki bunlar toplam nüfusun % 25'ini oluşturmaktaydı- sokak gösterileri yapmasıyla başlayan olaylar 27 Nisan 2007 akşamı ping yoğunluğuyla siber saldırıya dönüşmüştür. Hizmet reddi saldırıları sonrasında Hükümet ve parlamento siteleri ile siyasal parti ve medya kuruluşlarına ait siteler hızla servis dışı kalmışlardır. "Ülkede IP'leri kontrol eden ve izleyen sistemlerin olmaması da tehdidi daha hissedilir hale getirdi. Saldırılara tek cevap verecek kurum ülkedeki e-seçimlerin alt yapısını kuran uzmanlardı. 28 Nisan'da zirve noktasına ulaşan saldırılar yavaş yavaş azaldı ve 3 Mayıs'ta aralarında ping taşması şeklinde tanımlanan saldırıların da olduğu kontrol edilebilir seviyedeki saldırılar başladı. Rusya'nın İkinci Dünya Savaşı'nda Nazi Almanya'sını yendiği gün olan 9 Mayıs'ta da botnet saldırıları başladı. 11 Mayıs'ta yavaşlayan bu saldırılar, 18 Mayıs'ta tekrar başladı ve 23 Mayıs'a kadar devam etti" (Bıçakçı, 2012). İkinci saldırı dalgasında ülkenin iki büyük bankası olan 'Hansabank' ve 'SEB' internet üzerinden hizmet

veremez hale gelmiştir. Pek çok Rus sitesi kullanıcılarını basit programlarla saldırıya teşvik etmiş, kanal genişliğini doldurmak amacıyla ping saldırılarının nasıl yapılacağı detaylı olarak anlatılmıştır. Kullanıcıların bilgisi dışında ele geçirilmiş zombi bilgisayarların bir merkezden hedefe doğru saldırı için yönlendirilmesi şeklinde özetlenen botnet saldırıları ve 'bat' uzantılı dosya oluşturarak e-posta ve alan adı sunucularını (*domain name server – dns*) çökertme girişimleri en yaygın yöntemler olarak karşımıza çıkmıştır (Bıçakçı, 2012; Kara, 2013).

Estonya'nın maruz kaldığı saldırılara yönelik IP'ler yakından incelendiğinde veri paketlerinin ABD, Kanada, Rusya, Türkiye, Almanya, Belçika, Mısır, Vietnam gibi ülkelerden yönlendirildiği; saldırılara karşı önlem olarak bant genişliğinin 2 Gbps'den 8 Gbps'e çıkarıldığı; Estonya Savunma Bakanı Aaviksoo'nun tüm tedbirlerin yetersiz kalması nedeniyle NATO'yu göreve çağırması ve oluşturulan geçici (*ad hoc*) yardım gruplarının ilk siber savunma ordusu olarak anlam kazanması sürecin devam eden aşamaları olmuştur. Estonya'da yaşananlar özellikle Batı dünyasında terörizm ve finansal suçların dijitalleşmesi konularını gündeme getirmiş ve kapsamlı bir strateji geliştirilmesini zorunlu kılmıştır. Özellikle NATO'nun 2008 Bükreş Zirvesi'nde siber saldırılar ve kritik altyapıların güvenliği gibi sorunlara çözüm arayışları konusu gündeme gelmiş, siber savunmada işbirliği için birimlerin kurulması kararı alınmıştır. Bu karar kapsamında Brüksel merkezli Siber Savunma Yönetim Otoritesi (*Cyber Defence Management Authority*) ile Tallinn'in merkezli Siber Savunma İşbirliği Mükemmeliyet Merkezi (*Cooperative Cyber Defence Centre of Excellence*) kurulmuştur

Sonuç

Son çeyrek yüzyılda dünya ekonomisinde yaşanan dönüşüm ve bu dönüşüme paralel açığa çıkan yeni politik yapılanmalar, ulus devletlerin iç siyasetlerinin ve dış ilişkilerin çehresini de değiştirmiştir. Toplumsal yaşamın dünya genelinde yakınsadığı ve ülkeler arası ilişkilerin 'küreselleşme' olarak karakterize edilen bir sürece doğru yöneldiği son yıllarda, ulusal-uluslararası-global ekonomik ilişkilerin, siyasi güç dengelerinin ve kültürel unsurların yeniden biçimlenmesinin mümkün olduğu gözlemlenmektedir. Ulus devletleri tarihsel olarak dönüştüren küreselleşme eğilimi, güvenlik siyasetinde egemenliğin geçmişte olduğu üzere 'güçlü ordu-polis' anlayışından geçmediği; aksine 'etkin bir terörizmle mücadele stratejisi'yle mümkün olduğu yeni bir dönemi başlatmıştır. Siyasetbilimci F.Fukuyama'ya (2005) göre devlet olmaya ilişkin nitelikler aşınmakta ve yeni kurulan ya da yeniden organize olan pek çok küçük devlet siyasal istikrarasızlığa neden olmaktadır. Bu devletleri, çeşitli ulus-inşa şekilleri vasıtasıyla güçlendirmek, uluslararası güvenlik açısından hayati bir görev haline gelmiştir.

Uluslararası ilişkilerin tarihsel gelişimine bakıldığında, diplomasideki temel belirleyicinin 'ulusal çıkarlar' olduğu görülmektedir. İstihbarat toplama ve analiz etme anlayışı da tamamen bu ilke üzerine kurulu bir yapıda işlerlik kazanmaktadır. Son yıllarda ise bu yaklaşımda gediklerin oluşmaya başladığı ve uluslararası ilişkilerde dönemsel, stratejik ya da çokuluslu işbirliklerine, ulusalın ötesinde küresel tehditlere ve terör eylemlerini şekillendiren yeni güç aktörlerine de vurgu yapılmaya başlandığı bilinmektedir. İstihbarat faaliyetlerine ilişkin enformasyon, askeri ya da operasyonel nitelikli olmaktan çıkmış ve ekonomik, politik ve kültürel bir nitelik kazanmıştır: "Geçmişte de ülkeler, karşı taraf hakkında haber almak ve karşı tarafın gücünü, ordusunu, planlarını öğrenmek istemişlerdir ve casusluk bu düşünceyle başlamıştır. Son zamanlarda genel olarak bu anlamını yitirdi, çünkü ülkeler artık çok az savaşıyorlar. Üstelik bu konudaki bilgileri de teknolojik olarak elde ediyorlar. Şu anda büyük güçlerin yaptığı işler siyasi operasyonlardır ve bunlar ayrıca ekonomik olarak da desteklenir. Çok boyutlu operasyonlar yaparlar ve terör de bu operasyonların en önemli parçalarından biridir" (Kaynak, 2006). Uluslararası istihbaratın teröre karşı varoluşsal bir önem taşıyan ulusal-global enformasyon yönetimi stratejisinin bir parçası olduğu göz önünde bulundurulduğunda,

- Ülkelerin, karşı karşıya kaldıkları tehditlerle başa çıkabilmeleri için terörün 'amacının', 'kaynaklarının', 'bağlarının' ve 'iletişim tarzının' ne olduğunu çok iyi bilmeleri gerekmektedir.
- Global tehditleri ve riskleri hazırlayan ya da geliştiren koşulların çok yönlü olarak araştırılması ve terörün ilerde daha şiddetli bir konum kazanmasını önleyici tedbirlerin alınması önem taşımaktadır.
- Yeni uluslararası güvenlik yapısının, ülkeler arasında 'ulusal çıkar' temelinde örgütlenmesinden vazgeçilerek 'uluslararası güven ortamı' yaratacak 'global işbirliği' niteliğinde işlerlik kılınması sağlanmalıdır.

Uluslararası terörizmle mücadelede enformasyona erişim, bilgiye dönüştürme ve güvenlik politikası kapsamında küresel ölçekli kararlar verme süreci, otonom, sosyal yaşamdan soyutlanmış ve kendi operasyonelliği içine gömülmüş bir alan olarak algılanmamalıdır. Terörizmin ağ temelli yeni örgütlenmesi, onunla mücadelenin de zaman-insan tümleşmesinde yürütülmesini ve bu mücadelede enformasyondan azami yararı sağlayacak açık istihbarat tekniklerinin de yoğun biçimde kullanılmasını gerektirmektedir. Enformasyonu insan güvenliğinin aleyhine kullanan ya da kullanabilecek olan tüm güç odaklarını mental bakımdan hedefleyen siber istihbaratın, çağımıza damga vurması beklenen bir yönetim stratejisi olduğu açıktır.

Kaynakça

Bıçakçı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler*, 9 (34), 205-226

Bıçakçı, S. (2013). *21. Yüzyılda Siber Güvenlik*. İstanbul: İstanbul Bilgi Üniversitesi Yayınları

BBC (2016). 'Bir internet cumhuriyeti: Estonya', http://www.bbc.com/turkce/haberler/2016/05/160504_estonya_internet

Castells, M. (2005). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür Cilt I: Ağ Toplumunun Yükselişi.* (Çev.) E. Kılıç. İstanbul: İstanbul Bilgi Üniversitesi Yayınları

Hever, R. J. Jr. (1999) *Psychology of Intelligence Analysis.* Washington D.C: Center for the Study of Intelligence Publications.

Fukuyama, F. (2005). *Devlet İnşası.* (Çev.) D. Çetinkasap. İstanbul: Remzi Kitabevi.

Kara, M. (2013). Siber Saldırılar – Siber Savaşlar ve Etkileri. İstanbul Bilgi Üniversitesi SBE Bilişim ve Teknoloji Hukuku ABD. Yayımlanmamış Yükseklisans Tezi. İstanbul.

Kaynak, M. (2006). *Sil Baştan.* İstanbul: Timaş Yayınları.

Keane, J. (2010). *Şiddet ve Demokrasi.* (Çev.) M. Üst. Ankara: İmge Yayınları.

Knight-Jadczyk, L. ve Quinn, J. (2006). *9/11: The Ultimate Truth.* Canada: Red Pill Press.

Kumar, K. (2004). *Sanayi Sonrası Toplumdan Post-Modern Topluma*. (Çev.) M. Küçük. Ankara: Dost Yayınevi.

McQuail, D. ve Windahl, S. (1997). *Kitle İletişim Modelleri*. (Çev.) K. Yumlu. Ankara: İmge Yayınları.

NTV (2017). 'Sanal Para Birimine İlk O Ülke Geçiyor', http://www.ntv.com.tr/galeri/teknoloji/sanal-para-birimine-ilk-o-ulke-geciyor, BNYtMm01EEyShlEOB6Wsqg/ GDhlrfRs9EKt4I_GGCCecg

Ross, A. (2017). *Geleceğin Endüstrileri*. (Çev.) M. Buğan. Ankara: Orion Yayınları.

Singer, P.W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs To Know*. London: Oxford University Press.

Taylor, P. M. (2003). *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day.* New York: Manchester University Press.

Törenli, N. (2004). *Enformasyon Toplumu ve Küreselleşme Sürecinde Türkiye*. Ankara: Bilim ve Sanat Yayınevi.

Wiener, N. (1975). *Emek, Sibernetik ve Toplum*. (Çev.) İ. Keskin. İstanbul: Özgün Yayınları.

EBYS'lerde Bilgi Güvenliği Yaklaşımı ve TS 13298 Güvenlik Özellikleri

Abdullah KESKİN
Türk Standartları Enstitüsü

İnan ÖZKAN
Türk Standartları Enstitüsü

Öz

Her geçen gün daha fazla bilgi ve belge sayısal ortamlarda üretilmekte veya sayısal ortamlara aktarılmaktadır. Bilgi ve belgelerimizi ürettiğimiz, sakladığımız ve yönettiğimiz sayısal ortamların bilgi güvenliğine yönelik tedbirlerin alınması büyük bir gereklilik arz etmektedir. Gerçek ve tüzel kişilere ait yerine göre hizmete özel, gizli, çok gizli veya kişisel bilgi içeren belgelerin yönetildiği elektronik belge yönetim sistemlerinde bilgi güvenliğine yönelik çalışmaların yapılması da son derece önemli bir husustur. TS 13298 Elektronik Belge Yönetimi ve Arşiv Sistemi standardının 2015 revizyonu ile birlikte standarda EBYS ve arşiv sistemleri için alınacak güvenlik tedbirlerine yönelik gereksinimler eklenmiştir. Bu gereksinimler genel olarak EBYS ürünlerinin güvenlik testlerinin yapılması, arşiv sistemlerinde zaman damgası kullanımı ve şifreleme ve EBYS kullanılan kurum/kuruluşlar için TS ISO/IEC 27001 tavsiyeleri şeklindedir. TS 13298:2015 standardı içerisinde, yapılacak güvenlik testleri için uluslararası anlaşmalar çerçevesinde tanınırlığı olan ve tüm bilişim ürünlerine uygulanabilen TS ISO/IEC 15504 Ortak Kriterler standardından EAL 2 seviyesinde belgelendirme yapılması veya Ortak Kriterler standardına göre daha temel düzeyde güvenlik sağlanmasını amaçlayan TSE K 505 Temel Seviye Güvenlik Değerlendirmesi kriteri üzerinden güvenlik değerlendirmesi (testi) yapılması gerektiğinden bahsedilmektedir. Diğer taraftan arşive atılacak belgelerin zaman damgasıyla imzalanması arşiv malzemesinin bütünlüğünü korumak açısından önem arz etmektedir. Arşive aktarılacak olan belgelerin gizlilik derecesine göre şifrelenerek aktarılması ise arşiv malzemesinin gizliliği korumak açısından TS 13298 standardının istediği bir gereksinimdir. Ayrıca EBYS kullanan kurum ve kuruluşların TS ISO/IEC 27001 standardına uygun güvenlik tedbirleri alması gerektiği TS 13298 içerisinde tavsiye olarak verilmiştir. Bu çalışmada bilgi güvenliği ve ebys ilişkisi ele alınmış ardından TS 13298 standardının bilgi güvenliği özellikleri açıklanmıştır.

Anahtar Kelimeler: *TS 13298, Bilgi Güvenliği, EBYS lerde Güvenlik*

Giriş

Bilişim teknolojilerinin faydalarından her sektörde olduğu gibi belge yönetim süreçlerinde de faydalanılmaktadır. Elektronik imzanın yasal olarak kabul görmesi ile başlayan elektronik belge üretim süreci ülkemizde önemli ölçüde

yaygınlaşmış durumdadır. Yaygınlaşma ile birlikte bilgi güvenliği ile ilgili farkındalık eksikliği de çözüme kavuşturulması gereken bir sorun haline gelmiştir. Elektronik belge yönetim sistemi kullanan bir kurumda tasnif dışı ile çok gizli gizlilik dereceli belgeler aynı ortamda yönetilmektedir. Kurumun geleceğe aktarma gereği duyduğu tüm bilgi ve belgeler yine EBYS üzerinden yönetilmektedir. Elektronik belge yönetim sistemleri çalışma hayatını kolaylaştıran bilişim sistemleri olmalarının ötesinde kurumsal faaliyetlerin başlangıcından bitişine kadar tüm süreçlerin kanıtlarını da içeren önemli bir kaynaktır.

Bu nedenle elektronik belge yönetim sistemleri, kurumlarda kullanılan diğer bilişim sistemleri arasında güvenlik bağlamında da farklı bir konuma oturmaktadır. Performans, kullanılabilirlik ve öğrenilebilirlik gibi özellikler elektronik belge yönetim sistemlerinin temel gereksinimleri arasında sayılsa da öncelikli olarak güvenlik gereksinimi ön plana çıkmaktadır.

Bilgi güvenliği yaklaşımı ister yönetim sistemi bakış açısıyla olsun ister ürün güvenliği anlamında olsun temel 3 kavram üzerine kuruludur(TÜBİTAK BİLGEM):

- Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.
- Gizlilik: Bilginin yetkisiz kişilerin eline geçmemesidir.
- Erişilebilirlik: Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

EBYS ve Bilgi Güvenliği

TS 13298 standardının atıfta bulunduğu ve en çok bilinen ürün güvenlik standardı olan Ortak Kriterler standardı ve bilgi güvenliği yönetim sistemi standardı olan TS ISO/IEC 27001 standardı bilgi güvenliğini bahse konu 3 temel kavram üzerinden ele alır. EBYS'ler bilgi güvenliği açısından ele alındığında bütünlük, gizlilik ve erişilebilirlik kavramları göz önünde tutulmalıdır. EBYS'ler bünyesinde birçok varlık barındıran sistemlerdir. Bu nedenle bilgi güvenliği konusunu ele alırken öncelikle varlık analizi yapılması gerekir.

EBYS'lerde korunması gereken varlıklara örnek olarak Kullanıcı Hesap Bilgileri, Uygulamanın Kendisi, Belge ve Bileşenleri ile Günlük Kayıtları verilebilir. Varlık sayısı EBYS'nin geliştirme özelliklerine göre değişebilir. Örneğin belgelerini dosya sistemi üzerinde tutan bir ebys ile veritabanında tutan bir ebys'nin farklı varlık tanımları yapması muhtemeldir.

EBYS'nin örnek verilen varlıkları üzerinden gidilirse Kullanıcı Hesap Bilgileri varlığı için gizlilik önemlidir. EBYS de tanımlı olan kullanıcılara ait hesap bilgileri (kullanıcı adı ve parola) başka kişilerin eline geçmesi durumunda kullanıcılar adına işlemler yapılabilir. Bu durumda EBYS ve kullanıcıları zarara uğrayabilir.

Uygulamanın Kendisi varlık olarak ele alındığında erişilebilirlik önemlidir. EBYS'nin kullanıcılarına istenilen saatlerde kesintisiz hizmet vermesi beklenir. Hizmet aksatma (DoS) saldırıları veya farklı yöntemlerle sistemin hizmet dışı kalması işlerin aksaması, para ve prestij kaybı gibi istenmeyen sonuçlara yol açabilir.

EBYS'de bulunan Belge ve Bileşenleri varlığı için bilgi güvenliğinin 3 temel kavramı da önemlidir. EBYS içerisindeki belgelerin bütünlüğünün bozulması delil teşkil ettiği faaliyetin yanlış yürütülmesi, kişi ve kurumların zarara uğraması gibi sonuçlara yol açabilir. EBYS içerisinde bulunan özellikle gizlilik derecesi «tasnif dışı» üzerinde bulunan belgelerin yetkisiz kullanıcılar tarafından görüntülenmesi ve ifşası kurumsal ve milli menfaatlerin zarara uğramasına ve kurumların prestij ve para kaybına yol açabilir. EBYS'ye erişimden farklı olan bu durumda saldırgan, veritabanından bilgileri silme ya da şifreleme (wannacry gibi) gibi yöntemlerle erişebilirliğin engellenmesine neden olabilir. EBYS bünyesinde bulunan belgelere zamanında ve tam erişimin aksaması zaman, para ve prestij kaybına yol açabileceği gibi kurum ve kişilerin hak kaybına uğramasına da sebep olabilir.

Günlük Kayıtları varlığı için de bilgi güvenliğinin 3 temel kavramı da önemlidir. Günlük kayıtlarının bütünlüğünün bozulması sistemde yapılan hareketlerin izlenebilirliğini engeller. Bu durumda yetkisiz hareketlerin kim tarafından yapıldığı gizlenerek sorumluların haksızlığa uğraması gibi sonuçlara yol açabilir. EBYS günlük kaydında bulunan bilgilerin yetkisiz kullanıcıların eline geçerek bu bilgilerin ifşa edilmesi kurum ve kişilerin zarara uğraması, kurumların para ve prestij kaybı gibi sonuçlara yol açabilir. Sistemde yapılmış olan yetkisiz faaliyetin kim tarafından yapıldığına zamanında ve tam erişimin sağlanamaması sorumluların hak kayıplarına neden olabilir.

TS 13298 Güvenlik Özellikleri

TS 13298(TSE, 2015) ülkemizde EBYS'nin gelişimine önemli katkılar sunmuş ulusal bir standardımızdır. Standart gelişimi içerisinde öncelikle EBYS fonksiyonlarını daha sonra performans ve işlevsellik testlerini ve son olarak arşiv fonksiyonları ve güvenlik testlerini kapsamı içerisine almıştır.

2009 yılında yapılan revizyonda güvenlik ile ilgili temel fonksiyonların olması standart içerisinde zorunlu kılınmıştır. Bunlar;

- Kimlik doğrulama işlemleri
- Erişim haklarının yönetimi
  - Roller
  - Gruplar
- E-imza
- Günlük kayıtlarının tutulması

2012 yılında yapılan güncellemeler ile bilgi güvenliğini dolaylı anlamda etkisi olabilecek performans testlerinin yapılarak uygulamaların yetenekleri ölçülmüş ve yaptırılacak fonksiyonel testler ile hatalar önlenmeye çalışılmıştır.

2015 yılında yapılan güncelleştirmeler ile diğer testlerin yanı sıra güvenlik testleri de zorunlu hale gelmiştir. Ayrıca zaman damgası fonksiyonunun bulunması ve arşiv sisteminde şifreleme işleminin yapılması zorunlu maddeler arasında yer almıştır. TS ISO/IEC 27001 bilgi güvenliği yönetim sisteminin kurulması da tavsiye edilmektedir. Zorunlu hale gelen güvenlik testleri için 3 seçenek sunulmuştur:

- Ortak Kriterler Belgelendirmesi
- Temel Seviye Güvenlik Belgelendirmesi
- Temel Seviye Güvenlik Testleri

Ortak Kriterler Belgesi tercih edilmesi durumunda EBYS Koruma Profili uyumu aranmaktadır. Bu koruma profili dokümanıyla sistemin sağlaması gereken güvenlik özellikleri belirlenmiştir. Belgelendirme kapsamında TSE Siber Güvenlik Belgelendirme Müdürlüğü'nden lisanslı bir laboratuvar ile güvenlik değerlendirmesinin yapılması gerekmektedir.

TSE K 505 Temel Seviye Güvenlik Kriteri, güvenlik hedefinin değerlendirilmesi, güvenlik fonksiyonlarının fonksiyonel testleri ve güvenlik testinden oluşmakta olup daha temel ve hızlı bir güvenlik değerlendirmesini amaçlamaktadır. Temel Seviye Güvenlik Belgesi tercih edilmesi durumunda öncelikle TSE Siber Güvenlik Belgelendirme Müdürlüğü'nden lisanslı bir laboratuvar ile güvenlik değerlendirmesinin yapılması gerekmektedir.

Temel Seviye Güvenlik Değerlendirmesi tercih edilmesi durumunda TSE Siber Güvenlik Belgelendirme Müdürlüğü'nden lisanslı bir laboratuvar ile güvenlik değerlendirmesinin yapılması gerekmektedir. Bu durumda alınacak olan "olumlu" güvenlik değerlendirmesi raporu TSE'ye sunulur.

Arşiv malzemesinin arşive kaydedilirken zaman damgasının kullanılması arşiv malzemesinin bütünlük ve erişilebilirlik kontrollerinin yapılmasında önem arz etmektedir.

TS 13298 standardı "seçilmiş arşiv belgelerinin test edilmiş ve belgelendirilmiş şifreleme sistemleri ile şifrelenmesini" istemektedir. Gizlilik derecesi yüksek olan arşiv malzemesi için şifreleme güvenlik fonksiyonu olarak gereklidir.

Ayrıca TS 13298 içerisinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi belgelendirmesi aşağıdaki konuları kapsaması sebebiyle tavsiye edilmiştir:

- Güvenlik Politikası
- Risk Değerlendirmesi
- Varlık Yönetimi

- İnsan Kaynakları Güvenliği
- Fiziksel ve Çevresel Güvenlik
- İletişim ve İşletme Yönetimi
- Erişim Kontrolü
- Bilgi Sistemleri
- Bilgi Güvenliği Olayları Yönetimi
- İş Sürekliliği Yönetimi
- Uyum

Sonuç

Gerçek ve tüzel kişilere ait yerine göre hizmete özel, gizli, çok gizli veya kişisel bilgi içeren belgelerin yönetildiği EBYS'lerde bilgi güvenliğine yönelik çalışmaların yapılması son derece önemli bir husustur. Hem EBYS uygulamalarının kendileri için hem de kullanıldıkları ortam ve kurumlarda güvenlik önlemleri alınmalıdır. EBYS uygulamaları için güvenlik testleri mutlaka yapılmalıdır. Kurum ve kuruluşlarda TS 13298 standardına uygun EBYS'lerin kullanılması, standardın gereksinimleri çerçevesinde güvenlik önlemlerinin alınması ve TS EN ISO/IEC 27001 standardı kapsamında bilgi güvenliği yönetimi sağlanması önem arz etmektedir.

Kaynakça

TÜBİTAK BİLGEM, *Bilgi Güvenliği Ne Demektir?*, 08.12.2017 tarihinden adresinden erişildi.

TSE, *TS 13298 Elektronik Belge ve Arşiv Yönetim Sistemi*

EBYS (e-BEYAS) ve e-Arşiv Uygulamalarında Teknik Altyapı Boyutu ve Felaketten Kurtarma Merkezi (FKM): Ankara Üniversitesi Deneyimi

Barış OKUMUŞ
Mühendis
Ankara Üniversitesi Bilgi İşlem Daire Başkanlığı

Sadık KILIÇ
Sistem Yöneticisi
Ankara Üniversitesi Bilgi İşlem Daire Başkanlığı

Giriş

Ankara Üniversitesi iş süreçlerinde üretilen belgelerin ve yazışmaların çağın gerektirdiği nitelikte ve etkin bir biçimde güvenli sistemlerde yasal ve idari düzenlemelere uygun olarak elektronik ortamlarda üretilmesi ve arşivlenmesi amacıyla web tabanlı, ölçeklenebilir, diğer uygulamalar ile birlikte çalışabilen, e-imza destekli Elektronik Belge Yönetimi ve Arşiv Sistemi (e-BEYAS)'nin kurulması hedeflenmiştir.

Ankara Üniversitesi Elektronik Belge Yönetimi ve Arşivleme Sisteminin hizmet verdiği veri merkezlerinde kullanılan ve konumlandırılan tüm altyapı ve donanım varlıklarında e-BEYAS hizmet kesintilerini en aza indirmek amacıyla yedeklik, olası sorunlar esnasında veri kayıplarının önlenmesi ve verinin güvenliği ve gizliliği öncelikli olarak göz önünde bulundurulmuştur. Ankara Üniversitesi ve TÜRKSAT arasında işbirliği protokolüyle başlayan süreç, kademeli olarak donanım, yazılım ve altyapı bileşenlerinin satın alınması, iyileştirilmesi ve yeniden yapılandırılmasıyla ilerlemiştir.

Belgelerin elektronik ortamda üretilmesi, zaman ve mekan bağımsız bir şekilde erişilebilir olması, herhangi bir felaket sırasında veri kayıplarını önleyebilecek ve en kısa sürede tekrar erişilebilir hale gelecek şekilde depolanması, verinin birden fazla kopyasının farklı fiziksel konumlarda ve donanımlarda bulundurulması ve verilerin yedeklenmesi süreçlerinin kesintisiz ve güvenilir bir şekilde sürdürülebilmesi için 4 yılı aşkın zamandır Ankara Üniversitesi Belge Yönetim

Sisteminde kullanılan veri merkezleri teknik altyapısı, yöntem ve yaklaşımlar ve bu planlamaya dayanak oluşturan ihtiyaçlar ele alınmıştır.

Tasarlanan veri merkezi e-BEYAS'ın kullanıma alındığı tarihten bugüne geçen süre boyunca kesintisiz bir şekilde iş sürekliliği ve performans ihtiyaçlarını karşılamıştır. Tüm katmanlarda yedekli alt yapı ve donanım bileşenleri kesinti yaşanmadan planlı donanım bakımları yapılabilmesine olanak vermektedir. Sistem gözlemlenebilir ve ölçeklenebilir yapısı nedeniyle gelecekte oluşabilecek kapasite ve performans ihtiyaçlarına cevap verebileceği öngörülmektedir.

e-BEYAS Çalışmaları

Ankara Üniversitesi ve TÜRKSAT A.Ş arasında 9 Aralık 2011 yılında yapılan işbirliği protokolü sonrasında 2 Mart 2012 tarihinde Ankara Üniversitesi Belge Yönetim Sistemi çalışmalarına başlandı. Gereksinimlerin belirlenmesi ve gereksinimlere uygun planların hazırlanması, mevcut bilgi işlem kaynaklarının analiz edilmesi, planlanan donanımların ve yazılımların lisanslarının temin edilmesi, kurulum ve uyum testleri süreçlerinin tamamlanmasıyla 16 Eylül 2013 tarihi itibariyle e-BEYAS uygulaması Ankara Üniversitesinde kullanılmaya başlandı. e-BEYAS her yönüyle gözlemlenerek 16 Ekim 2014 tarihinde Felaketten Kurtarma Merkezi devreye alınmıştır. Süreç 2015 yılında yük dengeleme sistemi, disk depolama sistemleri, kesintisiz güç kaynakları, güvenlik duvarları ve ağ altyapısı modernize edilerek ilerletilmiştir. 2017 yılında Tandoğan veri merkezi iklimlendirme ve elektrik ünitelerinin iyileştirilmesi ve Felaketten kurtarma merkezi ikinci elektrik hattının tahsisi ile bugünkü haline getirilmiştir.

Veri Merkezleri Teknik Altyapı

Veri Merkezleri Elektrik Altyapısı

Tandoğan ve Gölbaşı FKM veri merkezleri yedekli elektrik hatlarından güç almaktadır. Veri merkezleri elektrik kesintileri esnasında otomatik devreye girebilen iki ayrı ve bağımsız jeneratör ve kesintisi güç kaynağı üniteleri ile beslenmektedir.

Veri Merkezleri Ağ Altyapısı

Tandoğan veri merkezi internet erişimleri ULAKNET ana hattı üzerinden gerçekleştirilmektedir. Veri merkezinde omurga ve kenar anahtarlar ikişer adet ve birbirlerini yedekleyecek şekilde konumlandırılmıştır. Ayrıca ULAKNET hattında kesinti yaşanması durumunda başka bir servis sağlayıcı üzerinden otomatik olarak devreye giren yedek internet bağlantısı tahsis edilmiştir. Yine aynı şekilde Tandoğan-Gölbaşı (FKM) veri merkezleri arasındaki veri transferleri için ana ve yedek arka hatlar olmak üzere iki ayrı hat tahsis edilmiştir.

Tandoğan Veri Merkezi

Ankara Üniversitesi Elektronik Belge Yönetim Sistemi Bilgi İşlem Tandoğan Veri Merkezi üzerinden hizmet vermektedir.

Yük Dengeleme Sistemi

Birbirini yedekleyecek şekilde aktif/pasif çalışan iki adet yük dengeleme donanımı kullanılmaktadır. Kullanıcıların bilgisayar ve mobil cihazları vasıtasıyla sisteme eristikleri ilk noktadır. İstemci ile sistem arasında oluşturulan şifreli ağ bağlantısı yük dengeleyici üzerinde sonlandırılır (SSL sonlandırma). Kullanıcılardan gelen erişim istekleri kullanıcıya en hızlı hizmet vermesi olası uygulama sunucusuna Least Connection algoritması ile yönlendirilir. Kullanıcıların veya saldırganların yük dağıtıcı arkasında çalışmakta olan sisteme doğrudan erişimleri güvenlik duvarı ile engellenmiştir. Yük dengeleyiciden geçen istekler ağ katmanı üzerinden uygulama sunucularına yönlendirir.

Ağ Sistemi

Tüm sistem donanımları veri iletimlerini 10g hızında fiber ve yedekli kablolar üzerinden gerçekleştirmektedirler. Belge yönetim sistemlerinin sağlıklı ve performanslı çalışabilmesi için yüksek hızda veri iletimi önem arz eder. Özellikle verilerin yedeklenmesi ve yedekten geri dönüş süreçlerinde ağ altyapısı ihtiyaçlara karşılık verebilmelidir. Tandoğan veri merkezinde hem ağ cihazları hem de fiber bağlantı kabloları birbirlerini yedekleyecek ve aktif-aktif çalışacak şekilde yapılandırılmıştır.

Uygulama Sunucuları

Ankara Üniversitesi Belge Yönetim Sistemi (e-BEYAS) uygulaması her biri 192GB RAM, on altışar çekirdekli 2 işlemciye sahip fiziksel uygulama sunucusu üzerinde çalışmaktadır. Her bir sunucu bulunan ağ, san ve güç kaynağı gibi bileşenler de ikişer adet bulunmaktadır. Böylece olası bir kablolama ya da ağ cihazlarındaki donanım arizalarına karsı yedeklik hedeflenmiştir. Sunuculara hem fiziksel olarak hem de ağ üzerinden bağlantı kurabilecek kişiler sadece yetkilendirilmiş kişiler olmalıdır. İstemciden gelen istekler yük dağıtıcıya ve sonrasında uygulama sunucuna ulaşır ve cevaplanır. Böylece kullanıcılar belgeler oluşturup çeşitli işlemleri gerçekleştirebilirler.

Veri tabanı Sunucuları

Gereksinimleri karşılayabilmek için iki fiziksel sunucu üzerinde çalışan bir veri tabanı küme yapısına ihtiyaç duyulmuştur. Bu ihtiyaç Oracle RAC "Oracle Real Applications Cluster" mimarisi ile sağlanmıştır. Oracle RAC tek bir veri tabanını birden fazla sunucu kümesinde çalıştırmak üzere etkinleştirir ve hiçbir uygulama değişikliği gerektirmeden hata toleransı, performans ve ölçeklenebilirlik sağlar. e-BEYAS uygulaması veri tabanları için 192GB RAM'li ve tüm bileşenleri

yedekli fiziksel sunucular konumlandırılmıştır. Veri tabanlarına veri tabanı yöneticileri haricinde erişim kısıtlanmıştır. Verinin kendisi fiziksel sunucu üzerinde değil, depolama üniteleri üzerinde bulunan disklerde muhafaza edilir. Böylece Veri tabanı boyutları arttıkça sisteme kolaylıkla kapasite artırımı yapılabilir.

SAN Anahtar

Veri tabanı sunucuları, depolama üniteleri ve yedekleme ünitesi (TAPE) arasındaki veri aktarımı sırasında, yüksek hızda veri aktarımı sağlayabilecek şekilde SAN anahtarlar yapılandırılmıştır. İki adet aktif-aktif çalışan SAN anahtarlar olası donanım ve kablo problemleri esnasında veri tabanları ile depolama ünitesi arasında yük hızda veri iletimi sağlamasının yanında hizmet kesintisi yaşanmaması için yedekli konumlandırılmıştır.

Veri Depolama Sistemleri

Belge yönetim sistemi verilerinin yüksek okuma yazma hızlarına sahip depolama sistemleri üzerinde saklanması önemli bir gereksinimdir. Bu nedenle e-BEYAS üzerinden üretilen belgelerin güvenli bir şekilde depolanması ve verilere yüksek hızda erişim ihtiyaçları öngörülerek ikişer denetleme birimi bulanan iki ayrı veri depolama sistemi konumlandırılmıştır. Veri depolama sistemleri aynı zamanda bilgi işlem bünyesinde verilen diğer hizmetler için de depolama ihtiyacını karşılamaktadır. Depolama sistemleri arasında blok tabanlı hacimlerde replikasyon yapılabilmektedir. Veri depolama sistemi üzerinde tekilleştirme (deduplication), thin provision, snapmirror, snaprestore gibi depolama ünitelerini verimli ve güvenli kullanma olanağı sağlayan yazılımlara ait lisanlar sağlanmış ve ayarlamalar yapılmıştır. Verilerin bir kopyası düzenli olarak ikinci depolama ünitesine aktarılır. Yedekler için tahsis edilmiş yine iki denetleyiciye sahip olan üçüncü bir veri depolama sistemi mevcuttur. Tüm veri depolama sistemleri tek noktadan izlenebilir ve performans ve kapasite raporları üretilebilir.

Kaset Yedekleme Sistemleri

Tüm veri tabanları ve sistemin isleyişinde rol alan sunucuların ve verilerin yedekleri alınmaktadır. İlgili yedekler yedekleme yazılımı vasıtasıyla önce yedekleme veri depolama ünitesine, daha sonra kaset ünitesi aracılığı ile kasetlere alınmaktadır. Kasetler belirli sürelerde bilgi işlemde bulunan ve yetkisiz erişimin kısıtlandığı kasada muhafaza edilir. Yedekleme ve yedekten geri dönüş senaryoları aralıklarla test edilmektedir.

VPN Erişim

Kullanıcılar e-BEYAS uygulamasına üniversite ağı içerisinden erişilebilirler. Sisteme Üniversite ağı dışından erişme ihtiyacı olan kullanıcılar bu taleplerini BEYAS Koordinatörlüğüne ilettikten sonra uygun görülmesi halinde gerekli

izinler verilerek VPN bağlantısıyla belge yönetim sistemine erişimleri sağlanmaktadır.

Sanallaştırma Sistemi

Ankara Üniversitesi Tandoğan veri merkezi sanallaştırma yapısı, fiziksel sunuculardaki donanım arızaları ya da performans gereksinimleri durumlarında e-BEYAS fiziksel sunucularının yerine kullanılabilecek şekilde planlanmış ve yapılandırılmıştır. Ayrıca e-BEYAS uygulamasının sürdürülebilirliği ve kullanılabilirliği konusunda önem arzeden test, demo ve eğitim uygulama sunucuları sanallaştırma kaynakları üzerinden yürütülmektedir. Kurum dışından gelen evrakların taranarak sisteme aktarılması için gerekli OCR yazılımı da sanallaştırma kaynakları üzerinden hizmet vermektedir.

Gölbaşı FKM Veri Merkezi

Ankara Üniversitesinde veri bütünlüğünü ve hizmet sürekliliğini etkileyebilecek felaketlerin gerçekleşme ihtimalini en aza indirmek için e-BEYAS uygulamasının çalıştırıldığı ana veri merkezi olan Tandoğan veri merkezinde mümkün olan en yüksek seviyede önlem alma yaklaşımı benimsenmiştir. Alınan tüm tedbirlere rağmen gerçekleşebilecek büyük ölçekli ve Tandoğan veri merkezini tamamen çalışamaz duruma getirebilecek bir felaket yaşanması durumuna karşı Gölbaşı kampüsünde Felaketten Kurtarma Merkezi (FKM) kurulumu yapılmıştır. Tandoğan veri merkezi kapsamında e-BEYAS uygulamasında üretilen tüm veriler, veri merkezini tamamen çalışamaz duruma getirebilecek olası felaket durumlarına karşı otomatik ve sürekli olarak Gölbaşı kampüsünde bulunan FKM veri merkezine aktarılır. Bu nedenle Gölbaşı FKM veri merkezinde de Tandoğan veri merkezinde bulunan benzer sistem modellemesi kullanılmaktadır. Ancak FKM veri merkezinde felaket sırasında donanım yedekliği belli ölçüde sağlanarak daha çok veri bütünlüğünü korumaya yönelik planlama yapılmıştır. Ayrıca kasete alınmış olan yedekler kilitli bir odada bulunan şifreli, yangına dayanıklı veri kartuş kasalarında saklanır.

Diğer Unsurlar

Hem Tandoğan hem de gölbaşı veri merkezinde donanımlara fiziksel erişimlerin denetlenebilmesi ve sistemlerin sürdürülebilirliğini sağlamak amacıyla İklimlendirme (Soğutma – Nem alma), Güvenli Kapı Sistemleri, Ortam İzleme Sistemleri, Kamera Sistemi, Yangın Algıma ve Söndürme Sistemi, Erken Uyarı ve Alarm Sistemi gibi unsurlar kullanılmaktadır.

Sayılarla e-BEYAS

Aralık 2017 tarihi itibari ile e-BEYAS sisteminde üretilen belge sayısı 4 milyonu aşmıştır. Üretilmiş olan belgelerin disklerde kapladığı toplam boyut 2.4TB ve veri büyüme miktarı yaklaşık olarak yıllık 0.5TB olarak gözlemlenmektedir. 4 yılı aşkın bir süredir kullanılmakta olan e-BEYAS Belge Yönetim Sistemi sayesinde binin üzerinde ağacın kurtarıldığı hesaplanmaktadır.

Bilgi, Teknik, Hukuk: Kişisel Verilerin Korunması[1]

Dr. Erkan AKDOĞAN

Ankara Üniversitesi Milletlerarası Hukuk Anabilim Dalı

Öz

Bilgi teknolojilerinin dönüşümüne koşut biçimde, e-devlet ve benzeri uygulamaların nitelik ve nicelik yönünden çeşitlenmesi sadece "birey"e değil "kamu"ya ilişkin sorunların da dönüşmesine neden olmaktadır. Öte yandan, bahsi geçen uygulamaların çeşitlenmesinin nedenlerinden biri olarak bireye veya kamuya ilişkin sorunların dönüşmesi de gösterilebilir. Anılan belirsizlik, özünde, birey ve toplumun nasıl kavrandığı, açıklandığı veya tasarlandığı ile doğrudan ilişkili görülmektedir. Söz konusu ilişkinin en belirgin örneklerinden birini "kişisel verilerin korunması" oluşturur. Bir yandan, kişisel verilerin korunması insan hakları söyleminin bir uzantısıdır. Logosentrik açıdan, korunması ihtiyacı hissedilen "kişisel veriler", kişinin, özel hayatın dokunulmazlığı gibi haklarla ilintili olarak onları tehdit veya ihlal eden bir sujeye ihtiyaç duyar ve anılan sujeden önce de vardır. Öte yandan, "kişisel veriler", kamu hukukuna ilişkin bir sorundur. Zira, yönetenin, yani sujenin, tanımı gereği, neyi veya kimi yönettiğini bilmesi gerekir ve bu amaçla sujenin sürekli bir biçimde bilgiye ihtiyacı bulunur. Ülkemizde 2016 yılında kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu, konuyla ilgili uluslararası andlaşmalar eşliğinde veya karşısında, yukarıda değinilen farklı bakış açıları ile okunduğunda; e-devlet ve benzeri uygulamaların hangi yöne doğru veya hangi bağlamda çeşitlendiği kadar değişmeyen, değişmeme eğilimi gösteren veya dönüşen sorunların da varlığı gösterilebilir. Çalışmamızda, böyle bir yol izlenerek 6698 sayılı Kanun ve uluslararası andlaşmaların özüne ilişkin yorum ve eleştiri getirilecektir.

***Anahtar Kelimeler**: Kişisel Verilerin Korunması, Hukukun Genel Teorisi, Kamu Hukuku, Uluslararası Andlaşmalar.*

Bilgi teknolojilerinin dönüşümüne koşut biçimde, e-devlet ve benzeri uygulamaların nitelik ve nicelik yönünden çeşitlenmesi sadece "birey"e değil "kamu"ya ilişkin sorunların da dönüşmesine neden olmaktadır. Öte yandan, bahsi geçen uygulamaların çeşitlenmesinin nedenlerinden biri olarak bireye veya kamuya ilişkin sorunların dönüşmesi de gösterilebilir. Anılan belirsizlik, özünde, birey ve toplumun nasıl kavrandığı, açıklandığı veya tasarlandığı ile doğrudan ilişkili görülmektedir. Söz konusu ilişkinin en belirgin örneklerinden birini

[1] Kısaltma ve atıflarda, aksi açıkça belirtilmedikçe "Bluebook" esas alınmıştır, bkz. **The Bluebook: a Uniform System of Citations**, Twentieth edition, Cambridge, The Harvard Law Review Association, 2015. Atıflarda, her bir eserin kaleme alındığı dilin kuralları izlenmiştir. Kısaltmalarda, doktrinde yaygın kullanılan kısaltmalar korunmuştur.

"kişisel verilerin korunması" oluşturur. Bir yandan, kişisel verilerin korunması insan hakları söyleminin bir uzantısıdır. Logosentrik açıdan, korunması ihtiyacı hissedilen "kişisel veriler", kişinin, özel hayatın dokunulmazlığı gibi haklarla ilintili olarak onları tehdit veya ihlal eden bir sujeye ihtiyaç duyar ve anılan sujeden önce de vardır. Öte yandan, "kişisel veriler", kamu hukukuna ilişkin bir sorundur. Zira, yönetenin, yani sujenin, tanımı gereği, neyi veya kimi yönettiğini bilmesi gerekir ve bu amaçla sujenin sürekli bir biçimde bilgiye ihtiyacı bulunur. Böylece (i) bir yandan yöneten ile yönetilen birbirinden ayrılarak yönetilenin birtakım hak ve özgürlükleri yönetenle ilişkilendirilmekte (*örn. insan haklarının sınırlandırılması*) (ii) öte yandan yönetenin yöneten niteliği yönetilene, yönetilenin haklarının varlığı ise tehdit ettiğine inanılan hakları yönetenin tanımasına, örneğin belli bir yönde eylemde bulunmasına bağlanmaktadır (*örn. sosyal ve ekonomik insan hakları*). Diğer bir anlatımla, ele alınan bağlama göre, yukarıda belirtilen suje ve objenin yeri, daha doğrusu kimliği değişmektedir. Yöneten açısından bakıldığında suje yönetendir, yönetilen açısından ise suje yönetilendir. Bununla birlikte gerek yöneten gerekse yönetilen açısından sujenin varlığı objeye bağlıdır.

Yukarıdakiler ışığında, çalışmamızı bölümlendirmeden ve kendisini bir önsöz veya giriş olarak görerek aşağıdaki hususlara işaret etmede yarar görüyoruz. Böylece "hukuk"a "Hukuk" niteliği veren düşünce yapısının anlaşılacağına inanıyoruz. Anılan nedenledir ki bu Tebliğde; doktriner tartışmalar içerisinde kimin doğru (*ὀρθόδοξος*) kimin yanlış görüşte (*ἑτερόδοξος*) olduğuna değinmek yerine başta her ikisine ve diğerlerine vücut veren görüşün (*δόξᾰ*) kendisini anahatlarıyla ortaya koymayı hedefliyoruz. Dolayısıyla, bir yandan *dogmatiğin-* veya *doktrinin-kendisine* diğer yandan *hukuk-un-felsefesine* dönük; eksikliği veya kusuru daha baştan belli bir tasarının daha yararlı olacağına inanıyoruz.

1.Hukuk doktrini veya doktrinin, kendisinin *hem* engeli *hem de* belirleyici şartı olan ve en az 2 (iki) yüzyıldır temel inceleme alanını oluşturan dogmatiğin (*=pozitif, müspet, olan hukuk*) dönüşümü yönünden, yukarıda değinilen sorunu farklı yönlerden göstermemiz, kavramamız mümkündür. Belirtilen yönden, uzun 19. yüzyıl başlarında *dogmatiğin* yeniden sorgulandığına tanık oluruz. Bugün, *dogmatik* genelde doktrinin bir vasfıyken anılan dönemde *dogmatiğin* çifte anlamda, *yani* hem pozitif, müspet, olan hukuk hem de anılanların, *mantıki çerçevede* sistematizasyonuna dönüştürüldüğüne inanıyoruz. Örneğin Kant'a göre ve özetle;

(i) Hukukçu, hukukun ne olduğunu (*was Rechtens sei/quid sit juris*), yani kanunların, geçmişte veya günümüzde belli bir yer ve zamanda ne dediğini söyleyebilir, ancak

(ii) aynı kuralların adil ve onların, adil olanla olmayanı (*iustum et iniustum*) ayırmaya yarar bir genel ölçüt (*allgemeine Criterium*) olup olmadığı soruları ondan saklanmıştır (*bleibt ihn wohl verborgen*);

(iii) yeter ki bir an (*eine Zeit*) bile bu ampirik ilkeleri (*jene empirischen Principien*) terk etmesin ve bu kararların kaynağını (*die Quellen jener Urtheile*), saf akılda (*in der blossen Vernunft*) aramasın;

(iv) gerçi ona, bu kanunlar rehberlik (*Leitfaden*) edebilirse de mümkün olan pozitif kanunların temelini oluşturmak amacıyla saf ampirik bir hukuk-doktrini (*"-" bilinçli kullanılmıştır*) (*sic*) "*sadece bir baş verir, güzel görünen, ama yazık! beyni olmayan bir baş*"[2].

2.Yukarıdaki anlatının özü; "maddi kaynak"ın kendisinin, yani hukuku ortaya çıkaran ve hukuk haline getiren şiddetin, hukuk-dışının, hukukçu tarafından araştırılmasının olanaksız, en iyi ihtimalle ek iş (*parergon*) olduğudur (=*yapamazsın çünkü yapmamalısın*), halbuki hukuku, "Hukuk" haline getiren, hukuku, hukukçunun işini tarif eden (*ergon*) budur (= *yapabilirsin çünkü yapmalısın*). Örneğin, bir özgürlüğün kullanımının kendisi genelgeçer kanunlara uygun özgürlüğe karşı bir ihlal, yani bir haksızlık (*unrecht*) oluşturuyorsa buna karşı şiddet kullanımı (*Verhinderung eines Hindernisses der Freyheit*), aynı kanunlara uygun olur (*recht*): Şiddete verilen izin, dar anlamda hukukla (*ius strictum*) ilgiliyken biri, daha geniş anlamda bir hukuku (*ius latium*) da düşünebilir, ilki haktır ama şiddet içermez (*Billigkeit*) diğeri şiddet içerir ama haksızdır (*Notwendigkeit*)[3].

Hukuk emir ve yasaklar bütünü ise, daha üstün olan yasak, yani esas yasaklanan (=*Yasak*), hukukun kendisi (=*Hukuk*) üzerine düşünmek, onu sorgulamak, kanunkoyanı veya çerçeveyi, Hukuk'u tartışmaktır . Böyleyse, anılan yönden, hukuki alan (*le champ juridique*), kanaatimizce, ilahiyat ve sanat ile aynı yapısal nitelikleri, aynı karakteristiği taşır. Yazılı olan söze, kitap derse, reel irreele, suje objeye, barış savaşa, olağan olağanüstüye, düzen anarşiye, iradi gayrı-iradiye, resmi özele, hukuk hukuk-dışına, kural ihlaline, doğru yanlışa, hakim azınlığa bağlanır; bağlanan, bağlanılan, bağ, bağlam tartışılamaz (*hipersembolizm*). Doktrin dahil her toplumda, bazıları tarafından ihlal edileceği bilinerek konulan yasaklar kadar kullanılmamak üzere verilen haklar da vardır: Tartışılması halinde Hukuk-Yasak'ın dışına çıkılır; hak kullanılmaması kaydıyla tanınmıştır[4]. Nitekim

---

[2] *id.*, **Metaphysische Anfangsgründe der Rechtslehre**, Königsberg, F. Nicolovius, 1797, §B, S. XXXII ("*Eine blos empirische Rechtslehre ist... ein Kopf, der schön seyn mag, nur Schade! dass er kein Gehirn hat*").

[3] KANT (1797), §D, S. XXXV; Anhang, S. XXVIII.

[4] Yukarıda izah ettiğimiz görüş, özü itibariyle "dilbilimci-postyapısalcı-yapıbozumcu"yla "postmodern-psikanalist"in üzerinde görüş birliğine vardığı nadir hususlardan biridir, bkz. *e.g.* J.DERRIDA, **Préjuges: Devant la loi** *dans* J.-F. LYOTARD et al, **La faculté de juger**, Paris, Minuit, 1985, not. pp. 115, 119, 121-122 ("*...la loi est l'interdit... cela ne signifie pas qu'elle interdit mais qu'elle est elle-même interdite, un lieu interdit. Elle s'interdit et contredit en mettant l'homme dans sa propre contradiction: on ne peut arriver jusqu'à elle et pour avoir* rapport *avec elle selon le respect,* il faut ne pas, il ne faut pas *avoir rapport à elle,* il faut interrompre la relation. *Il faut n'*entrer en relation *qu'avec ses représentants, ses exemples, ses gardiens. Et ce sont des interrepteurs autant que des messagers. Il faut ne pas savoir qui elle est, ce qu'elle est, où elle est, où et comment elle se présente, d'où elle vient et d'où elle parle. Voilà ce qu'*il faut *au* il faut *de la loi*"); P.BOURDIEU, **Les juristes, gardiens de l'hypocrisie**

büyük ölçüde kendisi dışındaki doktrinin yansıması veya aktarımına dayanan Türk hukuk doktrininde (*akademi, yargı, bürokrasi/diplomasi*) de anılan yönlerde ve kişisel veriler hakkında örnek çoktur[5].

3.Buraya değin anlatılanlar, bağlamından kopuk, *kişisel verilerle*, genel olarak insan haklarıyla ilgisiz görünebilir. *Biz aksi kanaatteyiz*. Zira, bir kere, günümüzde, bilinmeyen bilinenlerin bilinen bilinenlere dönüştürülmesinin, bilinmeyen bilinmeyen veya bilinen bilinmeyenlere dikkat çekmekten daha değerli olduğuna inanıyoruz[6]. Kaldı ki belirtilen sorunun anlaşılmasının, "kişisel verilerin korunması"na uygulanabilir hukuk yönünden belirleyici öneme sahip olduğunu düşünüyoruz. Nitekim, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun amacı, bir yandan,

> "*kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak*"ken

Öte yandan;

> *kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.*" (m.1)

---

collective *dans* F.CHAZEL, J.COMMAILLE, **Normes juridiques et régulation sociale**, Paris, LGDJ, 1991, pp. 95-99, not. 96 ("*...cette sorte de tour de passe-passe..., par lequel le juriste donne comme fondé* a priori*, déductivement, quelque chose qui est fondé* a posteriori*, empiriquement...*"); G.DELEUZE, **Différence et Répétition**, 7e édition, Paris, PUF, 1993, not. p. 8 et séq. ("*...la généralité est de l'ordre des lois. Mais la loi détermine seulement la ressemblance des sujets qui y sont soumis, et leur équivalence à des termes qu'elle désigne. Loin de fonder la répétition, la loi montre plutôt comment la répétition resterait impossible pour des purs sujets de la loi – les particuliers. Elle les condamne à changer...*") veya S.ZIZEK, **For They Know Not What They Do**, 2nd edition, London, NY, Verso, 2008, pp. 95, n. 35; 203-209 (*"'Law' is'law'"*).

[5] Doktrinin öncüsü sayılabilecek örnek için bkz. N.BAŞALP, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin, 2004. Avrupa Birliği ("AB") veya Avrupa Konseyi yönünden, birincisinin Türk doktriniyle ilgisini, *günümüzde Türkiye'nin* (01.09.2016) *tarafı olduğu hatırda tutulmak kaydıyla* Konsey'in 108 sayılı Konvansiyonu üzerinden kuran örnek için bkz. C.KAYA, *Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*, 69 İÜHFM 317 (2011); (*108 sayılı Konvansiyon ve Eki Protokol için sırasıyla*) "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" (ETS No. 108), BKK no: 2016/8576, k.t. 29/02/2016, RG tarihi/sayısı: 17.03.2016/29656 ve eki Protokol (ETS No. 181), BKK no: 2016/8840, k.t. 09.05.2016, RG tarihi/sayısı: 24.05.2016/29721. KAYA, "*kanun koyucu*" ile neyi kastettiğini belirtmez, bkz. *ibid.*, s. 332. Sözleşme ile eş zamanlı olarak TBMM'de kabul edilen 6698 sayılı Kanun'un metni üzerine genel değerlendirme için bkz. M.TURAN, *Kişisel Verilerin Korunması*, 80 KALKINMA 2 (2016). Anayasamız yönünden "kişisel verilerin korunması"yla ilgili sorunlar hak. bkz. E.KÜZECİ, *Anayasal Bir Hak: Kişisel Verilerin Korunması*, 128 BİLİŞİM DERGİSİ 142 (2010). Feminist yönden konuya *in passum* değinen örnek için bkz. C.KÜPELİ, *Şiddet Mağduru Kadınların Unutulma Hakkı*, 22 MÜHF-HAD 229, 234 (2016). Sayıca sınırlı olmakla birlikte konu üzerine literatürün sayıca arttığı söylenebilir. Bununla birlikte literatürdeki ilgi, konunun giderek daha dar ve teknik açıdan incelenmesi karşısında sorgulanmaya muhtaçtır. Kaldı ki yukarıdaki görüşlerimiz kabul edilirse Hukuk-Yasak'ın sorgulanmaması yönünden literatürün tamamı aynı görüştedir.

[6] S.ZIZEK, *Philosophy, the "unknown knowns", and the public use of reason*, 25 TOPOI 137 (2006).

Diğer bir anlatımla, *kanaatimizce*, kişisel verilerin korunmasını düzenleyen Kanun; kişileri veya verileri değil kişisel verileri korurken, örneğin Kant'ın, *gerçek anlamını ortaya koyabilmek amacıyla* yeniden okunarak eleştiriye muhtaç anlayışı yerine eleştiriye muhtaç *ama Kant'ın anlatısından farklı olarak bize tartışılamaz, üzerine yorumda bulunulamaz* bir diğer anlayışı getirmektedir. Böylece çifte anlamda bir belirsizlikle karşılaşılır. Diğer bir anlatımla, kanunkoyan *–ki yalnızca TBMM'yi kastetmeyiz–*, kendisinin parçası olduğu düzenin ihlaline karşı tasarlanan insan haklarının diğer insanlar (*gerçek ve tüzelkişiler*) tarafından ihlaline karşı "regülasyon" getirerek Kant'ın yukarıda belirtilen görüşünü *–ortadan kaldırmamakta ama–* dönüştürmektedir. Buna göre, devlet, kişisel verileri ihlal edemez; kişisel veriler ihlal edilirse bu ihlal devlete atfedilemez. Öte yandan, kişisel verilerin korunması, günümüz için bir gerekliliktir. Korunması amacıyla herhangi bir "kural" getirilemezse kişisel verilerin diğer insan hakları (*temel hak ve hürriyetler*) ile bağlantılı olarak ihlali karşılıksız kalır.

4.Dolayısıyla, son tahlilde, Kanun'un içer(d)iği, bir yandan "regüle ettiği", diğer yandan "kurallaştırdığı" temel yaklaşım, insan haklarını ihlal eden insanların uyacakları usul ve esasların belirlenmesidir. Bununla birlikte kanun-koyucu, belirtilen usul ve esasları, diğer bir anlatıma *prosedürü* de doğrudan doğruya belirle(ye)mez, zira anılanların belirlenmesi, öngörülebilmesi olanak dışıdır. Bir diğer anlatımla, Hukuk-Yasak veya hipersembolizm yinelenir ancak yinelemenin kendisi yinelenenden farklılaşır. Kanun, konulması öncesindeki gerekler doğrultusunda hazırlanır ancak konulduktan sonra kendisine uygun bir biçimde veya kendisi dayanak alınarak geliştirilmeye olanak tanır: Kişisel Verileri Koruma Kurumu'na ("Kurum") duyulan gereksinimin başlıca nedeni, *kanaatimizce*, budur (6698 sayılı Kanun, mm. 3/1/g; 19 ved.).

AB Veri Koruma Direktifi, Avrupa İnsan Hakları Sözleşmesi veya Birleşmiş Milletler Genel Kurulu, Ekonomik ve Sosyal Konsey'in veya İnsan Hakları Konseyi/Komitesi'nin tavsiye kararlarında da benzeri bir durumun varlığını seziyoruz. Anılanlara mündemiç "regülasyon" ve "kural"larla, *bir yandan* kişisel verilerin korunması kişiler arası ilişkilere indirgenerek kamunun ilgi alanı dışına çıkarılıp ötelenmekte, *öte yandan* getirdiği usul ve esaslar (*örn. Kurum*) ile kişisel verilerin korunması yönünden getirilen "güvenceler"in belirlenmesi geleceğe bırakılmaktadır. Böyle anlaşılırsa, özetle, belirtilen yaklaşım özünde platonik, Kantçı..., *yani* felsefidir ancak yeterince felsefi değildir.

5.*Kanaatimizce* modern düşünce dünyasını şekillendiren şekillendirmelerin eleştirisi bir şey, anılanların eleştirisini takiben onların yerine eleştirilemeyen (*yeni kamu yönetimi, yönetişim vb. kavramlar aracılığı ile*) "eski" anlamlara "yeni" kavramlar türeterek bunları dillendirmek başka bir şeydir. Nitekim *en azından*, hukuk düzeninin kendisi yönünden, hukuk düzeninin içinden bakanların bir bölümü (*diğer bölümüyle farklı görüşte de olabilirler*) için, "*elektronik ortamların hukuki düzene dahil edilmesi*", *yani* hukuk düzeninde bir boşluk olduğunun ima edilmesi olanak dışıdır. Zira, hukuk düzeni, özellikle bireyin

toplumla ilişkisi yönünden "her şey"i kapsar (*bu yönden, hiçbir yerde olmadığı da söylenebilir*). Diğer bir anlatımla, *HEIDEGGER'in ifade tarzıyla*, dünyaya "hukuk" gözlüğüyle bakanlar için her sorun "hukuki"dir. Kişisel verilerin korunması yönünden de böyle olduğuna inanıyoruz. Böyle anlaşıldığında, *naif bir biçimde*, Anayasamızın *her ne kadar eleştiriye açık olsa da* temel hak ve özgürlüklerle ilgili hükümlerinde *kişisel verilerle ilgili düzenlemenin* (m. 20/3) *kendisi dahil, bir bütün halinde kavranıp uygulanması gerektiğine inanıyoruz*. Örneğin, Anayasamızın 2. maddesine göre,

> "*Türkiye Cumhuriyeti, toplumun huzuru, milli dayanışma ve adalet anlayışı içinde, insan haklarına saygılı, Atatürk milliyetçiliğine bağlı, başlangıçta belirtilen temel ilkelere dayanan, demokratik, laik ve sosyal bir hukuk Devletidir*".

Sonuç olarak, formel, *yani* gerek şekli, belli bir şekilde ortaya çıkan gerekse resmi, resmiyete dayanan hukuk kaynakları yerine önerilen deforme veya gayrı resmi (*örn. ISO standartları*) kaynaklar neler ise kendisine, farklı nedenlerle, başta Anayasa olmak üzere uygulanması olanağı bulunmayan bu sonuncu kaynakların hukuk düzenine mevcut haliyle dahil edilmesi, kişisel verilerin korunmasına ne ölçüde hizmet eder, edebilir? Mesele, *bize göre* tanınmak veya tanımlanmaktan ziyade, karşılıklı olarak hukuka ve felsefeye imkan tanıyan düşünce yapısının kendisidir. O anlamda ki *bilgi* (*ἐπιστήμη*), *teknik* (*τέχνη*) ve *kanun* (*νόμος*) kavranabilir ve eleştirilebilir hale gelsin. Diğer bir ifadeyle, sorunun çözümü, *yani* kişisel verilerin korunması bakımından hukuk-doktrini kadar hukuk-dışı alanların da sorumluluğu olduğuna inanıyoruz. *Bize göre*, belirtilen alandaki boşluk, hukuk düzeninde olduğu ima edilen boşluktan daha büyük, çarpıcı ve yıkıcı olabilir.

Kaynakça

BAŞALP, Nilgün, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin, 2004

CHAZEL, F., COMMAILLE, J., **Normes juridiques et régulation sociale**, Paris, LGDJ, 1991

DELEUZE, Gilles, **Différence et Répétition**, 7e édition, Paris, PUF, 1968

KANT, Immanuel, **Metaphysische Anfangsgründe der Rechtslehre**, Königsberg, F. Nicolovius, 1797

KAYA, C., *Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*, 69 İÜHFM 317 (2011)

KÜPELİ, Ceren, *Şiddet Mağduru Kadınların Unutulma Hakkı*, 22 MÜHF-HAD 229, (2016)

KÜZECİ, Elif, *Anayasal Bir Hak: Kişisel Verilerin Korunması*, 128 BİLİŞİM DERGİSİ 142 (2010)

LYOTARD, Jean-François et al, **La faculté de juger**, Paris, Minuit, 1985

TURAN, M., *Kişisel Verilerin Korunması*, 80 KALKINMA 2 (2016)

ZIZEK, Slavoj, **For They Know Not What They Do**, 2nd edition, London, NY, Verso, 2008

ZIZEK, Slavoj, *Philosophy, the "unknown knowns", and the public use of reason*, 25 TOPOI 137 (2006)

Hukuksal Zorunluluklara Bağlı Olarak Veri Korumaya Bakış Açısındaki Değişim

Yrd. Doç. Dr. Türkay HENKOĞLU

Adnan Menderes Üniversitesi Yönetim Bilişim Sistemleri Bölümü

Öz

Veri koruma konusu, bilgi güvenliği politikalarında teknik, idari ve hukuksal sorumlulukların sınırlarının belirlenmesinde en zorlu alanı oluşturmaktadır. Bu nedenle, kurumların elektronik bilgi varlıklarının korunmasına ilişkin projelerinde taahhütlerde bulunmaktan kaçındıkları konular arasında yer almaktadır. Her ne kadar son yıllarda bu konuda yapılan çalışmalarla konunun önemine dikkat çekilmeye çalışılsa da, hukuksal çerçevenin daha belirgin hale gelmesi ile birlikte veri korumaya ilişkin sorumlulukların benimsenmeye başlandığı görülmektedir. Ancak bununla beraber, kurumların bu konuya gösterdikleri hassasiyetin en önemli ölçüsü olarak görülen ve kişi hakları çerçevesinde veri sahiplerinin görmeyi arzuladığı aydınlatma yükümlülüğünün yerine getirilmesi konusunda önemli eksiklikler bulunmaktadır. Siber güvenlik, ağ güvenliği vd. teknik alt bilgi güvenliği önlemlerini öne çıkaran kurumların, veri koruma hukuku çerçevesinde yerine getirmek zorunda olduğu bilgilendirmeyi yapmadıkları görülmektedir. Bu durum bilgi güvenliği zincirinin önemli halkalarından biri olan veri koruma konusunda uygulama eksikliklerinin bulunduğunu göstermektedir. Aydınlatma yükümlülüğünün yerine getirilmesi hukuksal bir zorunluluk olmanın yanı sıra, veri sahiplerinin ilgili kuruma olan güvenlerinin artmasını sağlamaktadır. Aynı zamanda, hangi verileri topladığını, bunları nasıl kullandığını ve veri sahiplerinin veri toplama, depolama ve işleme eylemlerini etkilemek açısından sahip oldukları seçenekler hakkında bilgilendirme yapan kurumların, kişisel verilerin korunmasına yönelik vermiş olduğu öneme ve almış oldukları güvenlik önlemlerini hukuksal yükümlülükler kapsamındaki sorumluluk bilinciyle almış olduklarına ilişkin çıkarımda bulunulabilmektedir. Bu çalışmada, bilgi güvenliği süreçlerinde bütünlüğünü sağlayan ve aynı zamanda kişisel hakların korunması açısından büyük önem taşıyan veri koruma hukukundaki gelişmelere bağlı olarak ortaya çıkan yeni yükümlülüklere dikkat çekilmesi amaçlanmıştır. Çalışma kapsamında 182 üniversitesin 6698 Sayılı Kişisel Verilerin Korunması Kanunu sonrasında konuya bakışları, faaliyetleri ve veri sahiplerini aydınlatma yükümlülüğüne yaklaşımı incelenmiştir. Yapılan araştırmada, üniversiteleri yasal yükümlülükleri yerine getirme ve bildirimde bulunma konusunda zorlayan uygulamaların bulunduğu ve bu nedenlere bağlı olarak da sorumlulukların yerine getirilemediği görülmektedir. Veri depolama ortamlarının bulunduğu yerler, kurum içi veri transferinde kullanılacak araçlar, veri işleme politikaları ve veri erişim yetkilendirmelerinin bu çerçevede öncelikli olarak gözden geçirilmesi gerekmektedir. Bununla beraber, aydınlatma yükümlülüğünün yerine getirilmesine yönelik olarak görülen eksikliğin giderilmesi amacıyla, çalışma sonunda tüm üniversiteler tarafından kullanılabilecek kısa bir bilgilendirme metni örneği ve başvuru formu örneği oluşturulmuştur.

Anahtar Sözcükler: *Veri Koruma, Bilgi Güvenliği, Aydınlatma Yükümlülüğü.*

Giriş

Bilginin kaydedildiği ortamların bilişim teknolojilerinin gelişimine bağlı olarak değişmesi, bireylerin temas ettikleri her alanda kişisel verilerinin elektronik ortamlara kaydedilmesini onaylamak zorunda bırakmaktadır. Günlük yaşamda kargo şirketlerinden bankalara, sağlık kuruluşlarından e-devlet kapsamındaki tüm kamu kurum ve kuruluşlarına kadar birçok alanda kişisel veriler işlenmektedir. Bu veriler, kamu yararına faaliyet gösteren kurumların elektronik arşivlerinde de diğer faaliyet bilgileriyle olan ilişkisi nedeniyle önemli oranda yer tutmaktadır. Kişisel verinin elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, açıklanması, aktarılması, yeniden düzenlenmesi, sınıflandırılması ya da kullanılmasının engellenmesi ve veriler üzerinde gerçekleştirilen her türlü otomatik işlemi içine alan bilgi yönetim süreçleri, hukuksal çerçevede "kişisel verinin işlenmesi" olarak tanımlanan kapsam içinde yer almaktadır (6698 Sayılı Kanun, 2016; Avrupa Adalet Divanı, 2003; Avrupa Konseyi, 1981, 2016; Kişisel Verileri Koruma Kurumu, 2017a). Bu nedenle bilginin elektronik ortamdaki yolculuğu esnasında, arşiv işlemlerinin bir parçası olarak sabit diske aktarılma işlemi dahi, kişisel verinin işlenmesi açısından hukuksal sorumlulukların dikkate alınmasını gerektirmektedir. Dijital dönüşümün sağladığı hız ve kullanım kolaylığı ile orantılı olarak, risklerin daha kolay yöntemlerle daha yaygın hale gelmesi de kaçınılmaz olmuştur. Bu nedenle, kişisel verilerin korunmasına ilişkin hukuksal zorunlulukların gündeme geldiği her noktada, bu verilerin korunmasına yönelik bilgi güvenliği önlemleri ve idari sorumluluklar da sorgulanmaktadır.

Kişisel verilerin güvenliğinin ve gizliliğinin korunması, temel hakların korunması kapsamında yer almaktadır. Bu çerçevede verilerin korunması, veri ile ilişkili olan bireylerin kişisel hak ve özgürlüğünün korunmasını hedef almaktadır (Anayasa Mahkemesi, 2008; Şimşek, 2008). Veri koruma konusunda alınacak önlemlerden bahsederken, hemen hemen tüm veri grupları içinde yer alan ya da bir bilginin (tarihsel olaylar vb.) hangi koşullarda oluştuğunu açıklarken başvurulan temel bilgi kaynakları içinde kişisel veriler yer almaktadır. Söz konusu veriler "kişisel veriler" olduğunda ise, kişisel hak ve özgürlükler açısından hukuksal sorumlulukların da dikkate alınması gerekmektedir (Anayasa Mahkemesi, 2008). Bu nedenle veri koruma konusuna verilen önem arttıkça ve alınacak önlemler detaylandırıldıkça, bu konunun hukuksal tarafında yapılması gerekenlere ilişkin liste uzamaktadır.

Kurum ve kuruluşlardaki veri sorumlularının veri koruma konusunda daha bilinçli olmalarını ve bu konuda veri sahiplerine taahhütte bulunmalarını sağlayan neden, kuşkusuz 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) içerisinde yer alan aydınlatma yükümlülüğüne ilişkin düzenlemedir (6698 Sayılı Kanun, 2016). Farklı bir açıdan bakıldığında ise, KVKK çerçevesinde bilgilendirme yükümlülüğünün yerine getirilmemesi TCK'nın 135., 136., 137. ve 138. Maddeleri (TCK, 2004) ile yapılan düzenlemelerin de daha etkin kullanımını

sağlayacak ve veri koruma yükümlülüklerini yerine getirmeyen kurum ve kuruluşlar daha fazla yaptırıma maruz kalabileceklerdir.

KVKK öncesinde yapılan araştırmalar, kişisel hakların korunması kapsamında kişisel verilerin korunmasına yönelik farkındalığın, önlemlerin ve bu konudaki çalışmaların yeterli düzeyde olmadığını göstermektedir (DDK, 2013; Henkoğlu, 2015). KVKK sonrasında ise e-posta, SMS ve müşteri ilişkileri aracılığıyla kişisel verilerin korunmasına yönelik olarak yapılan bildirimlerin günlük yaşam içinde artması, tüm çevrelerde bu konu hakkındaki farkındalığın oluşmaya başladığını göstermektedir. Bir başka yaklaşımla; hukuksal düzenlemeler bu konuya yaklaşımda belirgin olarak iyileşme sağlanmasına katkı sunmaktadır. Her ne kadar veri korumaya yönelik olarak alınan önlemlerin etkinliğinin ölçülmesi mümkün olmasa da, kurum ve kuruluşların bu konudaki sorumluluklarının bilincinde olmaları ve sorumluluklarının farkında olduklarını veri sahibi ile paylaşmaları önemli bir aşama olarak nitelendirilebilir.

Aydınlatma Yükümlülüğünün Önemi

Elektronik ortamda saklanan bilginin yayılma hızı ve bireyler için içerdiği hayati riskler dikkate alındığında, Anayasa'nın 20. Maddesinde[1]açık olarak tanımlanan veri koruma ve bilgilendirilme hakkı (T.C. Anayasası, 1982) bireylerin kişisel haklarının korunması açısından büyük önem taşımaktadır. Bununla beraber, KVKK içinde tanımlanan aydınlatma yükümlülüğü, Kanunun 28. Maddesinin 2. Fıkrasında tanımlanan belirli istisnalar dışında yerine getirilmesi gereken yükümlülüklerden biridir. Aydınlatma, veri sorumlusu için bir borç olarak anlam kazanırken, veri sahibi için bir haktır. Aydınlatma yükümlülüğünün yerine getirilmesi veri sahibinin kişisel hakkını kullanabilmesine imkân sağlamakla birlikte, idarenin veri işleme ve koruma konusunda şeffaf olduğunun da önemli bir göstergesidir.

Bilgi hukuku ve veri koruma mevzuatı göz önüne alındığında en önemli ve ilk göze çarpan konu başlıklarından biri olarak "rıza şartı" dikkati çekmektedir. KVKK'nın 5. Maddesinin 2. fıkrasında tanımlanan istisnalar dışında, kişisel verilerin ilgili kişinin açık rızası[2] olmaksızın işlenemeyeceği belirtilmektedir(6698 Sayılı Kanun, 2016). Bir irade beyanı olan açık rızanın kişinin özgür iradesi ile gösterilebilmesi için, veri sahibinin neye rıza gösterdiğini

[1]**(Ek fıkra: 7/5/2010-5982/2 md.)** Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Buhak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veyasilinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancakkanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

[2] KVKK, Madde:3; Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.

bilmesi gerekir. Bu nedenle, KVKK'da önemle vurgulanan açık rızanın gösterilme durumu, aydınlatma yükümlülüğünün yerine getirilmesi ile doğrudan ilişkilidir. Bu çerçevede değerlendirildiğinde, veri sahibine yönelik bilgilendirmenin veri işlemeyle ilgili tüm aşamalarını kapsayacak nitelikte olması gerekmektedir.

Veri korumanın etkin olarak yapılabilmesi için, başlangıçtan itibaren (data protection by default) ve tasarımdan itibaren veri koruma (data protection by design) yaklaşımının benimsenmesi önem taşımaktadır. Bu yaklaşımın AB'nin veri koruma mevzuatında veri koruma direktifi gibi (Avrupa Konseyi, 1995) birçok düzenleme içinde benimsendiği görülmekle birlikte, kavramsal olarak güncel AB Genel Veri Koruma Tüzüğü'nde (General Data Protection Regulation - GDPR) de (Avrupa Konseyi, 2016)daha kuvvetli bir şekilde yer aldığı görülmektedir. Düzenlemede bu kavramların açık olarak ifade edilmesi, veri koruma yükümlülüğünün ilk aşamadan itibaren yerine getirilmesinin gerektiğini ve dolaylı olarak veri sahibinin bilgilendirilmesinin de bu çerçevede yerine getirilmesi gereken en öncelikli yükümlülüklerden biri olduğunu göstermektedir.

KVKK, aydınlatma yükümlülüğü ve veri koruma yükümlülüğü için veri sorumlularını işaret etmektedir. Bu nedenle, bir kurum ya da kuruluşta KVKK'nın ne kadar dikkate alındığı veya başka bir ifade ile veri korumanın hukuksal koşullara uygun olarak yapılıp yapılmadığının anlaşılabilmesi için, veri sorumlusunun faaliyetlerinin gözlenmesi doğru bir yaklaşım olacaktır. Bu faaliyetler içerisinde en belirgin ve kolay ulaşılabilir olanı ise, hukuksal zorunluluklar çerçevesinde yapılan veri sahiplerine yönelik bilgilendirmedir. Bu konuda öncelikle kişisel verilerin işlenme şartlarının açık olarak tanımlanması, veri sahiplerinin sahip oldukları hakların tanımlanması ve bu çerçevede sorumlulukların belirlenmesi gerekmektedir.

Aydınlatma Yükümlülüğüne İlişkin Sorumluluğun Belirlenmesi

Veri güvenliğinin sağlanması ve aydınlatma yükümlülüğüne ilişkin sorumluluğun KVKK'nın 10. ve 12. Maddelerinde "veri sorumlusu" üzerinden tanımlandığı görülmektedir (6698 Sayılı Kanun, 2016). KVKK'nın 12. Maddesi gereğince veri sorumluları verinin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek için gerekli her türlü teknik önlemi almanın yanı sıra, idari tedbirleri de almakla yükümlüdürler. Bu nedenle KVKK çerçevesinde veri güvenliği ve aydınlatma yükümlülüğüne ilişkin olarak, ilgili kişilerin haklarını veri sorumlusuna karşı ileri sürebilecekleri anlaşılmaktadır. Bununla beraber, aydınlatma yükümlülüğü ve veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi halinde uygulanacak idari para cezasına ilişkin düzenleme KVKK'nın 18.Maddesinin 1. Fıkrasında yapılırken, devam eden 2. Fıkrada öngörülen cezanın veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri

hakkında uygulanacağı ifadesi kullanılmıştır. Aynı maddenin 3. Fıkrasında da eylemlerin kamu kurum ve kuruluşlarında gerçekleşmesi halinde ilgili kişiler hakkında disiplin hükümlerine göre işlem yapılacağı belirtilmiştir.

Aydınlatma yükümlülüğü ve veri güvenliğinin sağlanmasına yönelik sorumluluğun tayini konusunda en fazla tereddüt edilebilecek husus, veri sorumlusu ile veriyi işleyenin belirlenmesi ve bunlar arasındaki ilişkiye bağlı olarak sorumluluğun kime ait olduğuna açıklık kazandırılmasıdır. KVKK gerekçeleri ile birlikte analiz edildiğinde veri sorumlusunun yükümlülüklerinin anlaşılır olduğu görülse de, bu konuda oluşabilecek tereddütlerin önüne geçilmesi için şu notların bilinmesinde fayda bulunmaktadır;

- KVKK'nın 3. maddesinin (ı) bendine göre veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir[3]. Aynı maddenin (ğ) bendine göre veri işleyen, veri sorumlusu adına verileri işleyen gerçek veya tüzel kişilerdir.Buna göre veri işleyenin veri sorumlusunun talimatlarını yerine getirdiğiaçıktır.
- Tüzel kişiliğin içerisinde bulunan veri işleme faaliyetlerinden sorumlu gerçek kişiler veri sorumlusu olarak nitelendirilemezler.
- Veri sorumlusunun tüzel kişi olması halinde, bu sorumluluk tüzel kişiliği temsil yetkisi bulunan kişi ya da organlar tarafından yerine getirilmelidir. Bu kişi ya da organlar, tüzel kişilik içinde veri sorumlusunun yükümlülüklerini yerine getirmek amacıyla farklı kişi veya kişiler görevlendirse dahi, bu görevlendirme tüzel kişiliğin veri sorumlusu yükümlülüğünü ortadan kaldırmaz ve ilgili kişiyi veri sorumlusu yapmaz.
- Dışarıdan hizmet veren ve veri sorumlusunun verdiği yetkiye dayanarak hareket eden şirketler, ilgili organizasyonun dışında olsalar dahi KVKK kapsamında "veri işleyen" olarak değerlendirilmektedir.
- Bir gerçek veya tüzel kişi farklı faaliyetlere bağlı olarak[4] aynı anda hem veri sorumlusu hem de veriyi işleyen kişi olabilmektedir.
- Kurul tarafından veri sorumluları siciline kayıt zorunluluğuna istisna getirilmediği sürece[5], sadece kendi çalışanlarına ilişkin kişisel veri işleyen bir şirket de KVKK kapsamında değerlendirilmektedir.

---

[3] Bu kişiler, gerçek kişiler olabileceği gibi, kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabilir.

[4]Örneğin, bir şirket kendi personeline ilişkin kişisel verileri işlerken veri sorumlusu, müşterisi olan şirketlere yönelik kişisel verileri işlerken veri işleyen durumunda olabilmektedir.

[5] KVKK'nın 16. maddesinin 2. Fıkrası gereğince, işlenen kişisel verinin sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle veri sorumluları siciline kayıt zorunluluğuna istisna getirilebilir.

Veri Sorumlusunun Aydınlatma Yükümlülüğü ve Veri Güvenliğine İlişkin Yükümlülükleri Nelerdir?

KVKK'da doğrudan veri sorumlusunun yükümlülükleri arasında bulunan aydınlatma ve veri güvenliğine ilişkin yükümlülükler Kanunun 10. ve 12. Maddelerinde düzenlenmiştir. Buna göre veri sorumlusunun bilgi vermekle yükümlü olduğu ya da başka bir ifade ile bilgilendirme metninde yer alması gereken hususlar şunlardır;

- Veri sorumlusunun kimliği,
- Elde edilen kişisel verilerin hangi amaçla işleneceği,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- Veri sahibinin veri sorumlusuna başvurması halinde, veri sahibinin haklarını düzenleyen 11 inci maddede sayılan diğer haklara ilişkin bilgilerdir[6].

Veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri ise şunlardır;

- Kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ve muhafazasını sağlamak için gerekli her türlü teknik ve idari tedbirleri almak zorundadır.
- Kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, söz konusu tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumluluğu bulunmaktadır.
- Kendi kurum ve kuruluşunda KVKK'nın uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak ya da yaptırmak zorundadır.
- Görevde ya da görevden ayrılmış olsa dahi, öğrenmiş olduğu kişisel verileri KVKK'ya aykırı olarak açıklayamaz ve işleme amacı dışında kullanamaz.
- Hukuka aykırı olarak kişisel verilerin başkaları tarafından elde edilmesi halinde, veri sorumlusu tarafından en kısa sürede veri sahibi ve Kurul'a bilgi verilmelidir.

Araştırmanın Kapsamı ve Yöntemi

Bu araştırma ile aydınlatma yükümlülüğünün yerine getirilmesine ilişkin mevcut durumun belirlenmesi, bu yükümlülüğün yerine getirilememesine neden olabilecek unsurların açığa çıkartılması, mevcut eksikliklerin giderilmesine yönelik temel uygulama çözümlerinin üretilmesi ve nihai olarak elde edilen bulgular neticesinde Veri Koruma Mevzuatı'na uygun bir bilgilendirme metni ile başvuru formu örneğinin sunulması amaçlanmıştır. Bu amaçla araştırmada,

[6] KVKK kapsamında üniversiteler tarafından kullanılabilecek bilgilendirme metni ve başvuru formu önerisi EK:A ve EK:B'de sunulmuştur.

aydınlatma yükümlülüğünün mevzuata uygun olarak yerine getirilip getirilmediği, yükümlülüklerin yerine getirilmesine etki eden uygulamaların varlığı ve veri korumaya yönelik yasal düzenlemelerin tartışıldığı ya da bilgilendirmelerin yapıldığı etkinliklere üniversitelerde ne ölçüde yer verildiğine ilişkin sorulara cevap aranmaktadır. KVKK'da aydınlatma yükümlülüğünün nasıl ya da hangi iletişim araçlarıyla yerine getirileceğine ilişkin bir hüküm bulunmamaktadır. Bilgilendirme metninin ilgili kurumun internet sayfası üzerinden yapılması yeterli olabilmektedir. Bu nedenle tüm kamu ve özel kurumlarının daha kolay ve hızlı bir iletişim aracı olan web sayfalarını öncelikli olarak tercih ettikleri görülmektedir. Çalışmada, veri koruma konusundaki hukuksal değişimin üniversiteler üzerindeki etkisi, hızlı ve en doğru sonuç alınabilecek aydınlatma yükümlülüğünün yerine getirilmesi yönüyle incelenmiştir. Üniversitenin KVKK sonrasında veri sahiplerini aydınlatma yükümlülüğüne yaklaşımı web sayfalarından elde edilen bulgulara bağlı olarak değerlendirilmiştir.

Çalışmada araştırma yöntemi olarak nitel araştırma yöntemi tercih edilmiş ve bilgilendirme metinlerinin varlığına ilişkin veriler Yükseköğretim Kurulu üniversite listesinde yer alan 182 üniversitenin web sayfasından toplanarak içerik analizi tekniği ile incelenmiştir. Böylece aydınlatma yükümlülüğünün yerine getirilmesi sürecinin doğal ortamı olan web sayfaları üzerinden elde edilen verilerin gerçekçi ve bütüncül bir yaklaşım ile incelendiği nitel bir süreç izlenmiştir (Yıldırım ve Şimşek, 2011). Verilerin elde edilme sürecinde aydınlatma yükümlülüğüne ilişkin bilgi ve belgelerin varlığının yanı sıra, üniversitenin veri koruma konusundaki tüm etkinliklerine ilişkin veriler de toplanmıştır. Aydınlatma yükümlülüğünün yerine getirilmesine ilişkin veriler ile veri koruma konusundaki diğer üniversite etkinlikleri (politikaların varlığı, sempozyumlar, eğitim seminerleri, uyarı mesajları, uygulama önerileri vd.) ayrı olarak içerik analizi yöntemiyle değerlendirilmiş ve mevcut durumda görülen eksikliklerin giderilmesine (ya da yanlış uygulamalara) yönelik kısa öneriler sunulmuştur. Araştırma esnasında aydınlatma yükümlülüğünün yerine getirilememesine neden olabilecek uygulamaların (kurum içi veri transfer araçları, veri erişim yetkilendirmeleri ve veri depolama ortamları) görülmesi üzerine, bu husustaki teknik ve hukuksal uygulama çözümlerine de kısaca değinilmiştir. Bununla beraber, çalışmanın odak noktasını oluşturan aydınlatma yükümlülüğünün yerine getirilmesi için gereken ve araştırma sonucunda büyük ölçüde eksik olduğu görülen bilgilendirme metni örneği ve başvuru formu örneği, tüm üniversiteler tarafından kullanılabilecek bir form halinde oluşturulmuş ve çalışma eki olarak sunulmuştur.

Üniversitelerde Aydınlatma Yükümlülüğünün Yerine Getirilmesine İlişkin Mevcut Durum ve Uygulamaya Yönelik Öneriler

KVKK ve bu kanunun dikkate alınıp alınmadığının önemli göstergelerinden biri olan bilgilendirme faaliyetleri kişisel verilerin en fazla işlendiği kamunun tüm

alanlarını kapsaması açısından ayrı bir öneme sahiptir. Mevzuatta bankacılık (5411 Sayılı Kanun, 2005)ve e-ticaret (6563 Sayılı Kanun, 2014)gibi belirli alanlara yönelik olarak KVKK öncesinde yapılmış düzenlemeler bulunmaktadır. Bu nedenle bu alanlarda faaliyet gösteren kurum ve şirketlerin web sayfaları incelendiğinde KVKK'ya da kısa sürede uyum sağlamış oldukları görülmektedir. Kişi hakları ve gizliliğin sıkça tartışıldığı sağlık alanında da ilgili bakanlık tarafından KVKK'nın uygulamasına ilişkin hukuksal düzenlemelerin (Sağlık Bakanlığı, 2016)hızla yapıldığı görülmektedir.

KVKK öncesinde yapılan kapsamlı çalışmalar, üniversitelerin ve devlet kurumlarının veri koruma konusuna genel olarak "bilgi güvenliği" ile sınırlı olarak baktığı ve bu kapsamda teknik boyutta alınacak önlemler için bilgi işlem merkezlerini görevlendirdiklerini göstermektedir (DDK, 2013; Henkoğlu ve Uçak, 2016). Detaylı bir veri koruma kanununun olmaması, bilgi politikalarının bulunmaması, mevzuat içerisinden seçilen sorumlulukların anlaşılamaması ve veri sahiplerinin yeterli ölçüde bilgi sahibi olmaması, KVKK öncesinde veri koruma konusundaki uygulama eksikliklerinin başlıca nedenleri arasında sayılabilir. KVKK öncesinde üniversitelerde en fazla kişisel verinin kaydedildiği üç daire başkanlığını kapsayan çalışmaya katılım sağlayan 44 daire başkanının %66'sının hukuksal düzenlemeleri yetersiz bulduğu, diğer %34'ünü oluşturan katılımcıların da bu konuda fikirlerinin olmadığı görülmektedir (Henkoğlu, 2015). Çalışmanın ayrıntıları, uygulamaya ve politika geliştirmeye yönelik eksikliklerin en önemli nedenleri arasında hukuksal düzenlemelerdeki yetersizliğin bulunduğunu ortaya koymaktadır.

Bu çalışma kapsamında üniversite web sayfaları üzerinden yapılan analizde,

- Bir üniversitede doğrudan kişisel verilerin korunması ve işlenmesine yönelik politika bulunduğu görülmektedir.
- İki üniversitede KVKK'ya ilişkin çalıştay ve konferans gerçekleştirilmiş ve uygulama süreçleri detaylı olarak irdelenmiş olmakla birlikte, aynı üniversitelerin web sayfalarında üniversitelerin konuya ilişkin uygulamaları hakkında bilgi ya da veri sahiplerine yönelik bilgilendirme metinlerine ulaşılamamıştır.
- İki üniversitede belirli ücretler karşılığında KVKK eğitimi yapılmış olmakla birlikte, aynı üniversitelerin web sayfalarında üniversitelerin konuya ilişkin uygulamaları hakkında bilgi ya da veri sahiplerine yönelik bilgilendirme metinlerine ulaşılamamıştır.
- Bir üniversitede öğrenci bilgilerine erişim ve kullanımına yönelik yönerge hazırlanmış ve yönergede kişisel verilerin tanımı yapılarak özel hayatın gizliliği kapsamında korunduğu belirtilmiştir.
- Bir üniversitenin BİDB web sayfasında, belirli bir süre içinde e-posta gönderim sayısına yönelik kısıtlılıktan etkilenmemek amacıyla, kullanıcıların üniversite hesabı ile sunucuları yurtdışında bulunan farklı

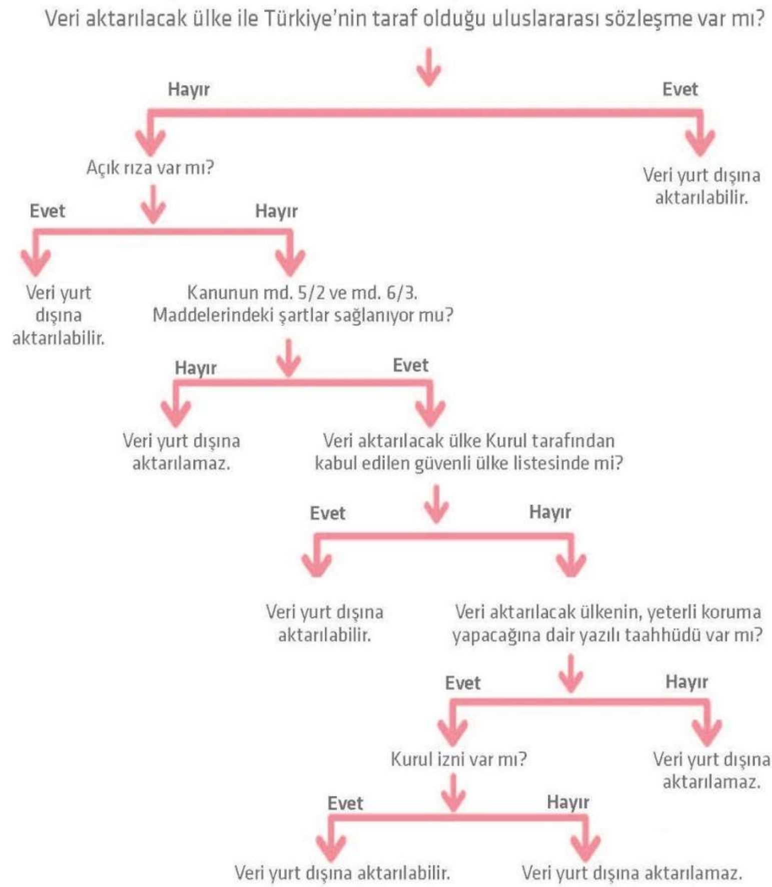
bir hizmet sağlayıcı üzerinden nasıl gönderim yapabileceğine ilişkin bilgi yer almaktadır. Bu bilgi içerisinde kullanıcıların verilerine yönelik risklerden bahsedilmemektedir. Üniversite e-posta uygulamalarına ilişkin benzer yurt dışı örnekleri (Boston University, 2017; Rochester University, 2012) incelendiğinde, bir e-posta kullanım politikasının bulunduğu ve bu politika içerisinde veri korumaya yönelik tüm hukuksal koşulların açıklandığı görülmektedir.

- Altı üniversitede KVKK'da öngörüldüğü gibi aydınlatma metninin yer aldığı ve veri sahiplerinin kişisel haklarının nasıl korunduğuna ilişkin yeterli düzeyde bilgi verildiği görülmektedir.
- Hastanesi bulunan altı üniversitenin web sayfasında, Sağlık Bakanlığı tarafından hazırlanan ve kişisel sağlık verilerini korumaya yönelik usul ve esasları düzenleyen "Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin[7]" bulunduğu görülmektedir.
- 42 üniversitenin yayınlamış olduğu dergilerde yapılan çalışmalarda ve etik kurul değerlendirme formlarında kişisel verilerin elde edilme süreçlerine ilişkin etik ve hukuksal koşullar hakkında bilgi yer aldığı ve içinde aydınlatma yükümlülüğüne yer verildiği görülmektedir. Ancak, çalışma kapsamında araştırılan bilgilendirme metni örneğinin bu üniversitelerin web sayfalarında bulunmadığı görülmektedir.

Üniversite web sayfaları üzerinden yapılan bu araştırmada, sayıca çok fazla olmamakla birlikte bazı üniversitelerin bilgi işlem merkezleri tarafından sağlanan hizmetlerin (e-posta vd.) dünya genelinde hizmet sunan bulut servis sağlayıcılar üzerinden verildiği görülmüştür. Bu hizmetlerin içinde kişisel verilerin yoğun olarak bulunduğu aşikârdır. Üniversitelere yönelik olarak sağlanan bu tür kurumsal e-posta adreslerinin sözleşmesi incelendiğinde ise, dünyanın herhangi bir yerinde ya da Türkiye'de herhangi bir kişinin aynı bulut servis sağlayıcı üzerinden ücretsiz olarak oluşturduğu hesabın gizlilik sözleşmesi ile benzer koşulları içerdiği anlaşılmaktadır. Bu durum, kişisel verilerin korunması açısından oluşabilecek risklerin (Balabit, 2017; Henkoğlu ve Külcü, 2013; Kauba ve Mayer, 2013) gerçekleşme olasılığının, gerekli bilgilendirmelerin yapılarak farkındalık oluşturulmaksızın kullanılması halinde ilgili üniversiteler için daha yüksek olduğunu göstermektedir. Bu tür uygulamaların, hem sunucularını Türkiye'de bulunduracağına ilişkin taahhütte bulunmayan bulut servislerinin güvenilirliği hem de bu durum hakkında veri sahiplerine yönelik bilgilendirme/uyarı yapılmaksızın aktif hale getirilmesi yönüyle KVKK uyumlu olmadığı görülmektedir. Otomatik olarak her personel için oluşturulan kurumsal e-posta vb. veri iletim ve depolama hesapları için KVKK'nın 9. Maddesinde tanımlanan açık rıza vd. şartların da gerçekleşmemiş olduğu açıktır. Üniversite

[7] Bilgi için Bkz.: http://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm

veri sorumluları, bazı hizmetleri devretmiş oldukları bu tür servis sağlayıcılara KVKK kapsamında belirlenmiş sorumlulukları devredememektedirler. Verilerin yurt dışına aktarılması sürecinde veri sorumluları tarafından dikkate alınması gereken aşamalar Kişisel Verileri Koruma Kurumu tarafından aşağıdaki şekil üzerinde gösterilmektedir (Kişisel Verileri Koruma Kurumu, 2017b).



Şekil 6: Verilerin yurt dışına aktarılması süreci

Bu çerçevede veri sorumlularının, kullanıcı hesaplarının oluşturulması esnasında kullanıcılara gerekli tüm bilgilendirmeyi yapmaları ve kullanıcının onayının alınması sonrasında hesabı aktif hale getirmelerinin hukuksal açıdan daha uygun olacağı değerlendirilmektedir. Hukuksal sorumluluklar çerçevesinde KVKK öncesinde işlenen verilere ve uygulamalara ilişkin olarak, KVKK'da iki yıllık

Kanuna uygun hale getirme süreci tanınmaktadır. Ancak etkin veri korumanın sağlanabilmesi için, kurum içi yazışmaların da içinde bulunduğu kurumsal faaliyetleri içeren elektronik belgelerin elektronik belge yönetim sistemleri (EBYS) üzerinden elektronik imza ile yapılması ve yurt dışındaki sunucular üzerinde işlenen verilere ulaşım açısından giriş kapısı niteliğindeki (kullanıcı doğrulama amacıyla kullanılan) yerel sunuculara yönelik erişim kontrollerinin en üst seviyede korunması önem taşımaktadır.

Değerlendirme ve Sonuç

Veri koruma hukukunda aydınlatma yükümlülüğü, veri sorumluları için yeni bir zorunluluğu ve yerine getirilmesi gereken yeni bir işlemi tanımlayan, veri sahibinin ise özel hayatının gizliliğinin sağlanmasına katkı sağlayan bir haktır. Bununla beraber, veri koruma hukukunun temel taşlarından biri olan kişinin irade beyanı olarak nitelendirilen rızanın gerçekleşmesi, veri sahibinin bilinçli olarak kendi kararını vermesine bağlıdır. Bunun için KVKK'da açık olarak tanımlanan aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir. Veri koruma ve aydınlatma yükümlülüğüne ilişkin hukuksal sorumluluklar KVKK ile birlikte çok açık bir şekilde ifade edilmektedir. Ancak üniversiteler üzerinden yapılan araştırma sonuçları, bu konuda yapılan çalışmalardaki artışa rağmen, uygulamaya yönelik yeterli düzeyde farkındalığın oluşmadığını ya da atılması gereken adımların atılmadığını göstermektedir. Üniversitelerin yanı sıra diğer kurum ve kuruluşlarda da bu konuya ilişkin farkındalığın ölçülmesi için kapsamlı çalışmalar yapılmalıdır. Veri sorumlularının KVKK kapsamında yerine getirmesi gereken sorumluluklar ve kişisel veri işleyen birimlerin uygulamalarına yönelik denetimleri hakkında yapılacak çalışmalar bu konunun bir bölümünü oluşturmaktadır. Diğer taraftan, veri sahiplerinin KVKK kapsamındaki haklarına yönelik bilinçlenme düzeylerini ölçen çalışmalara da ihtiyaç duyulmaktadır. Veri sahiplerinin farkındalığının ölçülmesine yönelik olarak yapılan çalışmalar, aynı zamanda bilinçlenme düzeyinin yükselmesine ve başvuru hakkının daha fazla kullanılmasına da katkı sağlayacaktır. Veri sorumlularının ve veri sahiplerinin hukuksal koşullardaki değişime bağlı olarak bilinçlendirilmesi için Veri Koruma Kurulu tarafından hazırlanacak bilgilendirme paketleri, kamu spotları vb. yayınların da daha aktif olarak kullanılması gerekmektedir. Belirli alanlarda (bankacılık vd.) oluşan farkındalığın tüm ülke geneline yayılabilmesi için, veri sahiplerinin de bu konuda daha bilinçli olmaları ve karşılaştıkları iyi örnekleri diğer veri sorumlularından beklemeleri sürecin daha sağlıklı ilerlemesine katkı sağlayacaktır.

Üniversitelerin bazı servisleri yurt dışındaki sunucularını kullanan bulut ortamlarına taşımak zorunda kalmalarının nedenleri arasında bütçe ve personel yetersizliği olduğu düşünülmektedir. Üniversitelerde bilgi işlem merkezlerini donanım maliyetleri ve personel iş yükü açısından zorlayan ve zaman zaman bu

yetersizlikler nedeniyle kullanılabilirliğe ilişkin problemlerin sıkça yaşandığı servislerin bulut ortamına taşınması en uygun çözüm olarak benimsenmektedir. Ancak içinde kişisel veri barındıran E-Posta vd. hizmetleri sunucularını Türkiye'de bulunmayan bulut servis sağlayıcıları üzerinden herhangi bir özel sözleşme yapmaksızın sunan üniversiteler, veri koruma ve aydınlatma yükümlülüklerinin yerine getirilmesi için daha fazla özen göstermelidirler. Üniversitelerde KVKK'da belirlenmiş veri koruma yükümlülüklerinin yerine getirilmesi ve bu korumaya ilişkin bilgilendirmenin yapılabilmesi için, verinin işlendiği ve saklandığı bilgi işlem teknolojilerine daha fazla kaynak ayrılmalı, bu teknolojileri işletebilecek yeterliliğe sahip ve yeterli sayıda personel görevlendirilmeli ya da belirli sözleşmeler çerçevesinde sunucularını Türkiye içinde bulunduran bulut servis sağlayıcıları ile uzun vadeli çözümler üretilmelidir. Üniversite akademik personelinin bu konu hakkında bilgilendirilmesinin yanı sıra, idari personelin de yazışmalarını sadece EBYS üzerinden yapmaları konusunda farkındalık oluşturulmalıdır. Sınır ötesine kontrolsüz olarak verilerin taşınmasına imkân sağlayan uygulamalar, ilgili kurumların sadece bilgilerinin çalınması risklerini taşımamaktadır. Elde edilen bu veriler belirli amaçlara bağlı olarak sınıflandırılarak ve arşiv haline getirilerek, ne zaman kötü amaçla kullanılacağı belirsiz bir risk unsuru haline de gelmektedir. Veri koruma ve aydınlatma yükümlülüğüne ilişkin olarak bu çalışma kapsamında görülen eksikliklerin nedenleri arasında, bu tür hizmet devirlerinin de olabileceği değerlendirilmektedir. Ancak bununla beraber, KVKK kapsamında yer alan yükümlülüklere karşı duyarsız kalınması, üniversite veri sorumlularının bu konudaki başarılarını daha iyi bir noktaya taşımamaktadır. Bu nedenle, veri sorumlularının ilk aşamada aydınlatma yükümlülüklerini yerine getirmeleri ve kullanıcıları mevcut risklere karşı uyarmaları, meydana gelebilecek zafiyetlerin önüne geçilmesi açısından önem taşımaktadır.

Aydınlatma yükümlülüğünün yerine getirilmediği ve kullanıcılar için tanımlanan kurumsal e-posta hesaplarının kullanıcılar tarafından "tam olarak üniversitenin kontrol, denetim ve güvenlik kalkanı" içinde yer aldığını düşündüğü altyapılar daha fazla risk içermektedir. Bu servislerin sağladığı kullanım kolaylığı ve yüksek performans, personelin kurumsal ve kişisel verilerin kurum içerisinde dağıtımını/gönderimini bu servisleri kullanarak yapmaya yönlendirmektedir. Mevcut KVKK'nın örnek alındığı 95/46 Sayılı AB Veri Koruma Direktifi'nin de bu konuda yetersiz kaldığının vurgulanarak, AB'nin yeni Genel Veri Koruma Tüzüğü'nde "başlangıçtan itibaren" ve "tasarımdan itibaren" veri koruma anlayışına açık olarak yer verilmesi, bu risklerin ilk aşamadan itibaren en düşük seviyede tutulmasının önemini açıkça ortaya koymaktadır.

Sunucuları yurt dışında bulunan e-posta hizmet sağlayıcıları üzerinden kurumsal e-posta adresi kullanılarak gönderim yapılabilmesi için, bu hizmet sağlayıcıların sisteminde kurumsal hesaba ilişkin bilgilerin (kullanıcı adı ve şifresi gibi) tanımlanması gerekmektedir. Bu durumda gönderilen e-posta içeriği ile birlikte, kurumsal e-posta bilgilerine yönelik riskler de oluşmaktadır. Bu tür uygulamalara

ilişkin yönlendirme yapılırken, kullanıcılar olası risklere karşı uyarılmalıdır. Bununla beraber, şifre doğrulama ve oturum açma işlemlerinin yerel bir sunucu üzerinden yapılması nedeniyle, bu sunuculara yönelik olarak yapılabilecek yetkisiz erişimlere karşı en üst seviyede güvenlik önlemleri alınmalıdır. Kullanıcı hesaplarını denetleyen sunucular mümkün olduğunca diğer sunuculardan (web sunucusu vd.) ayrı donanımlar üzerine tasarlanmalıdır. Kullanıcıların e-posta için kullanmakta olduğu şifreyi birçok farklı alanda kullanıyor olabileceği göz ardı edilmemelidir.

Üniversitelerin web sayfaları üzerinden yapılan araştırma sonuçları, KVKK'nın yürürlüğe girmesi ile birlikte birçok üniversitede konuya ilişkin bilinçlendirme çalışmalarının başladığı, tartışıldığı ve üniversite dergilerinde de bu konunun çok daha fazla yer aldığı görülmektedir. Bu durum KVKK öncesi ile kıyaslandığında, veri koruma konusundaki hukuksal koşullardaki değişimin kişisel verilerin ve ona bağlı olarak kişisel hakların korunmasına yönelik etkisi açık olarak görülebilmektedir. Ancak bu üniversitelerin birçoğunda, üniversitenin sorumluluğunu yerine getirmesi, kurumsal kullanıcıların bilgilendirilmesi ve haklarının hatırlatılmasına yönelik metinlere yer verilmediği görülmektedir. Bununla beraber, üniversitelerin teknik altyapı ve personel eksikliğinin, bu hukuksal sorumlulukların yerine getirilmesini zorlaştırdığı görülmektedir. Bu nedenle, öncelikle personel ve donanımsal eksikliklerin giderilerek kişisel verilerin Kanunda öngörüldüğü şekilde korunması ve bunun somut göstergesi ya da taahhüdü anlamına gelen bilgilendirmenin yapılması önem taşımaktadır. Kişisel verilerin korunması için gerekli önlemlerin alınması ve bilgilendirmenin yapılması hukuksal sorumluluklar içinde yer almakla birlikte, bilgi güvenliği zincirinin de en sağlam halkalarından birini oluşturmaktadır. Özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında kişisel verilerin korunmasını sağlama ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirme amacıyla KVKK kapsamında kurulan Kişisel Verileri Koruma Kurumu'nun çalışmalarının da takip edilmesi, eksikliklerin giderilmesi açısından önemlidir. Kurumun KVKK'nın uygulanmasına yönelik yayınlarının (Kişisel Verileri Koruma Kurumu, 2017a) veri sorumluları tarafından takip edilmesi ve bu çerçevede hazırlanan bilgilendirme paketlerinin kurum içinde kişisel verileri işleyen birimlere sunulması ile kurum içi uygulamaların hukuksal koşullara uyumlu hale getirilmesi sağlanabilecektir. Hizmet içi eğitim ve farkındalık oluşturma çalışmalarına ilâve olarak, veri sorumluları ya da onun adına görevlendirilen kişiler tarafından uygulamaların hazırlanan plan çerçevesinde kontrol ve denetiminin yapılması da önem taşımaktadır.

EK:A

KİŞİSEL VERİLERİN KORUNMASI KANUNU BİLGİLENDİRME METNİ

XYZÜniversitesi olarak kişisel verilerinizin korunması konusunda hassasiyet göstererek, Üniversite ile ilişkili tüm şahıslara ait kişiselverilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)'na uygun olarak işlenmesi ve muhafaza edilmesine önem vermekteyiz. Bu amaçla KVKK kapsamında tanımlı "Veri Sorumlusu" sıfatıyla, kişisel verilerinizi aşağıda açıklanan ve mevzuatta yer alan sınırlar çerçevesinde işlemekteyiz.

Üniversitemiz, KVKK uyarınca; Veri Sorumlusu sıfatıyla, işleme amacına uygun, sınırlı ve ölçülü olacak şekilde talep ettiği ve üniversitemizle paylaşmış olduğunuz kişisel verilerinizi, işlenmelerini gerektiren amaç çerçevesinde; kaydedebilir, depolayabilir, muhafaza edebilir, yeniden düzenleyebilir, kanunen bu kişisel verileri talep etmeye yetkili olan kurumlar ile paylaşabilir, KVKK'nın öngördüğü hallerde ve koşullarda, yurtiçi veya yurtdışı üçüncü kişilere aktarabilir, devredebilir, sınıflandırabilir ve KVKK'da sayılan şekillerde işleyebilir.

Üniversitemiz Tarafından Toplanan Kişisel Verilerin Hukuki Sebebi ve Yöntemleri Nelerdir?

Kişisel verilerinizin işlenmesine ilişkin hukuki sebepler, Üniversitemiz birimleri tarafından 2547 sayılı Yükseköğretim Kanunu ve ilgili ikincil mevzuat uyarınca hukuksal yükümlülüklerin yerine getirilmesi amacıyla, internet sitesi, sosyal medya ve benzeri vasıtalarla sözlü, yazılı ya da elektronik olaraktoplanan kimlik bilgilerinin (ad, soyad, doğum tarihi, adres, cep telefonu, e-posta adresiniz gibi kişisel veriler) kaydedilmesi, düzenlenmesi ve mevzuat, ilgili düzenleyici kurumlar ve diğer otoritelerce öngörülen bilgi saklama, raporlama, bilgilendirme yükümlülüklerine uymaktır. Kişisel verileriniz, aşağıda yer verilen amaçlar doğrultusunda hizmetlerin sunulabilmesi ve bu kapsamda Üniversitemizin sözleşme ve kanunlardan doğan sorumluluklarını eksiksiz ve doğru bir şekilde yerine getirebilmesi amacıyla Üniversitemiz tarafından otomatik ya da otomatik olmayan yöntemlerle toplanır.

Bilgileriniz Hangi Amaçla İşlenebilir ve Kimlere Aktarılabilir?

Kişisel verileriniz veri tabanları üzerinden listeleme, raporlama, analiz ve değerlendirmelerin yapılması, istatistiki bilgilerinüretilmesi ve gerektiğinde gizlilik koşullarına uymak kaydı ile bunlarınilgili uzmanlarla paylaşılması, internet sitemizi ve diğer iletişim kanallarımızı ne şekilde kullandığınıza dair analiz yaparak sizlere daha iyi hizmet sunulabilmesi, hizmetlerimize ilişkin kişisel seçim imkânlarının araştırılması ve geliştirilmesi, Üniversite faaliyetlerinin sizlere tanıtılması,yasal yükümlülüklerin veya yetkili idari kuruluşların taleplerinin yerine getirilmesi ve Üniversitemizin stratejilerinin belirlenmesi ve uygulanması amacıyla KVKK'nın 5. ve 6.Maddeleri çerçevesinde işlenecektir.

Toplanan kişisel verileriniz, gerekli güvenlik önlemlerinin alınması ile burada bahsedilen amaçların (Üniversitemizin tümfaaliyetleri için gerekli çalışmaların ilgili birimler tarafından yapılması, altyapı sağlayıcılar, Üniversitemizle iş ilişkisi içerisinde olankişilere ilişkin işlemler vd.) gerçekleştirilmesi için kanunen yetkili kurumlara(Kişisel Verileri Koruma Kurumu, Yükseköğretim Kurulu, Çalışma ve Sosyal Güvenlik Bakanlığı, Gümrük ve Ticaret Bakanlığı, Maliye Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu gibi kamu tüzel kişileri)

vefaaliyetlerin yürütülmesi amacıyla yapılan sözleşmeler çerçevesinde diğer 3. kişilere KVKK'nın 8. ve 9. Maddeleri çerçevesinde aktarılabilecektir.

Kişisel Verilerinizin İşlenmesine İlişkin Haklarınız Nelerdir?

Kişisel veri sahibi olarak, haklarınıza ilişkin taleplerinizi, aşağıda düzenlenen yöntemlerle Üniversitemize iletmeniz durumunda Üniversitemiz talebin niteliğine göre talebi en geç otuz gün içinde (Kişisel Verileri Koruma Kurulunca bir ücret belirlenmediği sürece) ücretsiz olarak sonuçlandıracaktır. Bu kapsamda kişisel veri sahipleri KVKK'nın 11. Maddesi gereğince;

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- KVKK'nın ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.

VKK'nın 13. maddesinin 1. fıkrası gereğince, yukarıda belirtilen hakların kullanılmasına ilişkin taleplerinizi, yazılı olarak (veya Kişisel Verileri Koruma Kurulu'nun belirleyeceği diğer yöntemlerle) Üniversitemize iletebilirsiniz. KVKK'nın 11. maddesi kapsamında belirtilen haklardan kullanmayı talep ettiğiniz hakkınıza yönelik açıklamalarınızı içeren yazılı başvurunuzu; www.xyz.edu.tr adresindeki formu doldurarak, formun imzalı bir nüshasını "XYZ Üniversitesi, İstanbul" adresine kimliğinizi tespit edici belgeler ilebizzat elden iletebilir, noter kanalıyla gönderebilir veya ilgili formu elektronik imzalı olarak iletebilirsiniz.

EK:B

XYZ ÜNİVERSİTESİ KVKK BAŞVURU FORMU

6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda ("KVKK") ilgili kişi olarak tanımlanan kişisel veri sahiplerine, KVKK'nın 11. maddesinde kişisel verilerinin işlenmesine ilişkin birtakım taleplerde bulunma hakkı tanınmıştır. KVKK'nın 13. maddesinin birinci fıkrası uyarınca; veri sorumlusu olan Üniversitemize bu haklara ilişkin olarak yapılacak başvuruların yazılı olarak veya Kişisel Verilerin Korunması Kurulu ("Kurul") tarafından belirlenen diğer yöntemlerle tarafımıza iletilmesi gerekmektedir. Kurul'un belirleyeceği diğer yöntemler belirlendikten sonra, bu yöntemler üzerinden başvuruların ne şekilde alınacağı Üniversitemizce ayrıca duyurulacaktır.

Bu çerçevede "yazılı" olarak Üniversitemize yapılacak başvurular, işbu formun çıktısı alınarak;

- Başvuru Sahibi'nin (kişisel veri sahibinin) şahsen başvurusu ile,
- Noter vasıtasıyla,
  - Başvuru Sahibi tarafından 5070 Sayılı Elektronik İmza Kanununda tanımlı olan "güvenli elektronik imza" ile imzalanarak tarafımıza iletilebilecektir.

Tarafımıza iletilmiş olan başvurularınız KVKK'nın 13. maddesinin 2. fıkrası gereğince, talebin niteliğine göre talebinizin bizlere ulaştığı tarihten itibaren otuz gün içinde yanıtlandırılacaktır. Yanıtlarımız KVKK'nın 13. maddesi hükmü gereğince yazılı veya elektronik ortamdan tarafınıza ulaştırılacaktır.

A. Başvuru Sahibi iletişim bilgileri:

Ad Soyad:	
TC Kimlik No:	
Telefon:	
E-posta:	
Adres:	

B. Lütfen Üniversitemiz ile olan ilişkinizi belirtiniz. *(Öğrenci, mezun, öğrenci veya mezun yakını, iş ortağı, çalışan adayı, eski çalışan, üçüncü taraf firma çalışanı gibi)*

☐ Öğrenci /Mezun ☐ Akademik Personel ☐ İdari Personel ☐ Eski Çalışan (Çalışılan Yıllar: ..-..) ☐ Üçüncü Kişi Firma Çalışanı	☐ Diğer ………… …………..
Üniversitemiz içerisinde iletişimde olduğunuz Birim:……………….……………………… Konu:……………….………………………	

C. Lütfen KVK Kanunu kapsamındaki talebinizi detaylı olarak belirtiniz:

…………………..…………….………………………….…………………………….
………...………………….....……………..……………………………….………………………
………..………...…………………...……………..……………………………….……………
………………….……….....……………….....……………..……………………………….…
……………………………..……….....……………….....……………..……………………………
……..………………………………..……….....……………….....……………..………………
………………..…………………………….………..…

D. Lütfen başvurunuza vereceğimiz yanıtın tarafınıza bildirilme yöntemini seçiniz:

- Adresime gönderilmesini istiyorum.
- E-posta adresime gönderilmesini istiyorum.

  (E-posta yöntemini seçmeniz hâlinde size daha hızlı yanıt verebileceğiz.)

- Elden teslim almak istiyorum.

  (Vekâleten teslim alınması durumunda noter tasdikli vekâletname veya yetki belgesi olması gerekmektedir.)

İşbu başvuru formu, Üniversitemiz ile olan ilişkinizi tespit ederek, varsa, Üniversitemiz tarafından işlenen kişisel verilerinizi eksiksiz olarak belirleyerek, ilgili başvurunuza doğru ve kanuni süresinde cevap verilebilmesi için tanzim edilmiştir. Hukuka aykırı ve haksız bir şekilde veri paylaşımından kaynaklanabilecek hukuki risklerin bertaraf edilmesi ve özellikle kişisel verilerinizin güvenliğinin sağlanması amacıyla, kimlik ve yetki tespiti için Üniversitemiz ek evrak (Nüfus cüzdanı veya sürücü belgesi sureti vb.) talep etme hakkını saklı tutar. Taleplerinize ilişkin bilgilerin doğru ve güncel olmaması ya da yetkisiz bir başvuru yapılması halinde Üniversitemiz, söz konusu yanlış bilgi ya da yetkisiz başvuru kaynaklı taleplerden dolayı sorumluluk kabul etmemektedir.

Başvuru Sahibi (Kişisel Veri Sahibi)

Adı Soyadı :

Başvuru Tarihi :

İmza :

Kaynakça

5411 Sayılı Kanun. (2005). Bankacılık Kanunu. 14 Eylül 2015 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5411.pdf adresinden erişildi.

6563 Sayılı Kanun. (2014). Elektronik Ticaretin Düzenlenmesi Hakkında Kanun. 14 Eylül 2017 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6563.pdf adresinden erişildi.

6698 Sayılı Kanun. (2016). Kişisel Verilerin Korunması Kanunu. 12 Eylül 2016 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf adresinden erişildi.

Anayasa Mahkemesi. (2008). Özel hayatın gizliliği ve korunması. 29 Kasım 2017 tarihinde http://www.resmigazete.gov.tr/eskiler/2008/06/20080625-8.htm adresinden erişildi.

Avrupa Adalet Divanı. (2003). *Bodil Lindqvist Kararı*.

Avrupa Konseyi. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 28 Kasım 2017 tarihinde https://rm.coe.int/1680078b37 adresinden erişildi.

Avrupa Konseyi. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 18 Eylül 2017 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF adresinden erişildi.

Avrupa Konseyi. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 19 Eylül 2017 tarihinde http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf adresinden erişildi.

Balabit. (2017). Understanding privileged identity theft. 17 Eylül 2017 tarihinde https://pages.balabit.com/rs/855-UZV-853/images/Balabit-Understanding-Privileged-Identity-Theft.pdf?mkt_tok=eyJpIjoiTVRrMU1XSmxabVE0TmpBMyIsInQiOiJmb1pXOGo2SlY5emN6UUNOUVJ6Qm5ucWxJYjZhRVFrWHYxYTF6ckgyU3lWT25NcjZ5MmhCOVU4cTVGUFIxd1wvV3BDVGk5YmN4SGdFVzI1Rys0ME5vQ0dnbkl4U1ZOOEZcL053UjZROFBsSDNaNm0wYmlpaFdNQ3RnS1UyNm5GTTR5OVlGcmp0cXBvelk2dmRMUlp0NmZmUT09In0%3D adresinden erişildi.

Boston University. (2017). *BU Google Apps Acceptable Use and Data Security*. 30 Eylül 2017 tarihinde https://www.bu.edu/tech/about/policies/google/ adresinden erişildi.

DDK. (2013). *Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*. Ankara: Cumhurbaşkanlığı Devlet Denetleme Kurulu.

Henkoğlu, T. (2015). *Bilgi güvenliği ve kişisel verilerin korunması*. Ankara: Yetkin Yayınları.

Henkoğlu, T. ve Külcü, Ö. (2013). Bilgi erişim platformu olarak bulut bilişim: Riskler ve hukuksal koşullar üzerine bir inceleme *Bilgi Dünyası, 14*(1), 62-86.

Henkoğlu, T. ve Uçak, N. Ö. (2016). Information Security and the Protection of Personal Data in Universities. *International Journal of Business and Management Invention, 5*(11), 30-43.

Kauba, C. ve Mayer, S. (2013). Data Condentiality and Privacy in Cloud Computing. 30 Eylül 2017 tarihinde http://www.uni-salzburg.at/fileadmin/multimedia/SRC/docs/teaching/SS13/SaI/Paper_Kauba_Mayer.pdf adresinden erişildi.

Kişisel Verileri Koruma Kurumu. (2017a). *Kişisel verilerin korunması kanunu ve uygulaması*. 29 Kasım 2017 tarihinde http://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf adresinden erişildi.

Kişisel Verileri Koruma Kurumu. (2017b). Kişisel verilerin turtdışına aktarılması. 6-7.13 Eylül 2017 tarihinde http://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20YURTDI%C5%9EINA%20AKTARILMASI.pdf adresinden erişildi.

Rochester University. (2012). University of Rochester Policy on Email Use. 30 Eylül 2017 tarihinde http://tech.rochester.edu/wp-content/uploads/2015/09/email-use-policy.pdf adresinden erişildi.

Sağlık Bakanlığı. (2016). *Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik*. 11 Eylül 2017 tarihinde http://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm adresinden erişildi.

Şimşek, O. (2008). *Anayasa Hukukunda kişisel verilerin korunması*. İstanbul: Beta Yayınevi.

T.C. Anayasası. (1982). Türkiye Cumhuriyeti Anayasası. 13 Eylül 2017 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf adresinden erişildi.

TCK. (2004). Türk Ceza Kanunu. 13 Eylül 2017 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf adresinden erişildi.

Yıldırım, A. ve Şimşek, H. (2011). *Sosyal bilimlerde nitel araştırma yöntemleri* (8. Baskı ed.). Ankara: Seçkin Yayıncılık.

Türk Hukuk Sisteminde Bilgisayar Araması ve Bulunan Delillere Elkonması

Yrd. Doç. Dr. Yavuz ERDOĞAN

Lefke Avrupa Üniversitesi
Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı

Özet

Günümüzde insanlar gerek özel hayatlarını gerekse iş hayatlarını bilgisayara taşımışlardır. Bu durumun doğal sonucu olarak suçların işlenme alanları ve hatta klasik suçların delillerinin saklanma alanları da bilgisayar ortamına kaymıştır. Bu durumda suçların tespiti ve delillere ulaşılabilmesi için bilgisayarlarda arama yapmak zorunluluk haline gelmiştir. Ancak bilgisayar üzerinde yapılacak aramalar, aynı zamanda kişilerin özel hayatına müdahale niteliğinde de olacağından, bilgisayarlarda yapılacak aramaların titizlikle yapılması ve mümkün olduğunca özel hayata müdahale etmemesi gerekmektedir. Bu kapsamda Türk hukuk sistemine bakıldığında bilgisayar aramasının Ceza Muhakemesi Kanunu'nun (CMK) 134. maddesinde düzenlendiğini görmekteyiz. Bu maddenin içeriğine baktığımızda ise, eleştirilebilecek pek çok hususun bulunduğunu görmekteyiz. Kanaatimizce CMK'nın 134. maddesi tümüyle değiştirilmelidir. Elimizde bulunan bu çalışmada, CMK'nın 134. maddesinin her bir fıkrasının ayrı ayrı değerlendirmesi yapılarak, çözüm önerileri sunulmuştur.

Anahtar Kelimeler: *Bilgisayarda Arama, Bilgisayarda Elkoyma**,** Ceza Muhakemesinde İspat**,** Dijital Delil**,** Hukuka Uygun Delil*

Summary

Nowadays, people mostly prefer to keep information and documents about their private and business life in computers. As a natural consequence, the computers have become the virtual fields where crimes are committed and evidences are hidden. Within this context, search of computers has become indispensable in order to investigate the committed crimes and hidden evidences. However, the criminal search on computers will somehow be considered as interference to people's private life, so any research should be made meticulously and should not interfere with anyone's private life as much as possible. Within this scope, as we look at the Turkish Judiciary System, it can be noticed that computer search is regulated in Article 134 of Turkish Criminal Procedure Code. Moreover, as the context of Article 134 is analyzed more vigorously, many aspects can found to criticize. In our opinion, Article 134 of Turkish Criminal Procedure Code should be changed completely. In this article, each and every clause of TCPC article 134 is analyzed, criticized proposed solutions are presented.

Key Words: *Search Of Computers, Computer Seizure, Evidence In Criminal Procedure, Digital Evidence, Legal (Justifiable) Evidence*

Giriş

Ceza muhakemesi hukukunun temel hedefi (soruşturma evresi dâhil), maddi gerçeği bulmaktır. Bu durumda delillerin toplanması ceza muhakemesinin en önemli olaylarından biridir. Nitekim Yargıtay Ceza Genel Kurulu da 10 Mayıs 2005 gün ve 2005/5-35 esas ve 2005/51 karar sayılı kararında *"Ceza yargılamasının amacı somut gerçeğin hiçbir kuşkuya yer vermeyecek şekilde saptanmasıdır. Bu nedenle derlenmesi gereken her tür kanıtın elde edilmesi ve değerlendirmeye konu edilmesi gerekir."* demek suretiyle delil toplamanın önemini vurgulamıştır. Ancak maddi gerçeğe ulaşmak amacıyla hareket edilirken insan hakları ve hukukun temel prensipleri ihlal edilmemelidir. Diğer bir deyişle, maddi gerçeğin ortaya çıkarılması her ne pahasına olursa olsun ulaşılması gereken, mutlak ve istinasız bir amaç değildir; temel hak ve özgürlüklere dokunmamak esastır.

Bu kapsamda baktığımızda inceleme konumuz olan bilgisayarda arama kurumu önem kazanmaktadır. Zira bilgisayarda arama yapılması halinde, insanların en yakınındaki kişilerden dahi sakladığı özel hayatının en derin kısmına, sır alanına girilmektedir. Günümüzde internetin sağladığı kolaylıklar dikkate alındığında, bu sır alan çok daha genişlemektedir. Bu durumda bilgisayarda yapılacak bir arama ile bireyin özel hayatın gizliliğine, haberleşme hürriyetine ve kişisel verilerine müdahale edilmiş olunacağından, bilgisayarda arama konusu kanunlarda düzenlenirken çok daha titiz davranılması gerekecektir. Nitekim İnsan Hakları Evrensel Beyannamesi'nin (İHEB) 12. maddesinde (m.) ve Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 8. maddesinde olduğu gibi, temel insan hakları metinlerinde herkesin özel hayatına saygı gösterilmesinin gerektiği açıkça düzenlenmiştir.

Bu doğrultuda bilgisayarda arama yapılmasına ilişkin olarak Türk hukuk sistemine baktığımızda, kanun niteliğindeki tek düzenlemenin Ceza Muhakemesi Kanunu'nun (CMK) 134. maddesi olduğunu; bu maddenin elektronik belgeler bakımından hiçbir güvence içermediğini, uzaktan erişim ve bulut teknolojileri bakımından uygulanması imkânının bulunmadığını görmekteyiz. Bu durum usulün belli olmaması nedeniyle soruşturma makamlarını zorda bıraktığı gibi, kişilerin hak ve özgürlükleri bakımından da tehlike yaratmaktadır. Zira soruşturma makamları pekâlâ uzaktan ve habersiz olarak arama yaparken, kişilerin özel ve hatta sır alanına girebilecektir.

Çalışmanın Amacı ve Yöntemi

CMK'nın 134. maddesini incelediğimizde, gerek insan hakları bağlamında gerekse teknik anlamda eleştirilebilecek çok fazla şey olduğunu, metnin yeni baştan düzenlenmesi gerektiğini gördük. Bu nedenle çalışma konusu olarak Türk hukuk sisteminde bilgisayar aramasını seçtik. Ancak aramanın vazgeçilmez sonucu olan elkonmanın da madde metninde bulunması nedeniyle, elkonma konusunu da çalışmamızda değerlendirdik.

Bu amaçla çalışmamızı kaleme alırken CMK'nın 134. maddesinde düzenlenen iki farklı arama şekli ve elkonma sistemini ayrı ayrı başlıklar altında değerlendirip, çözüm önerilerimizi sunduk.

Arama yapılması için benimsenen unsurlardan yola çıkarak arama şekillerinden birini (CMK m.134/5) "basit arama" olarak isimlendirdik. Basit arama hükmü önceden bilinen belirli bir unsurun arandığı (örneğin adı belli bir dosyanın arandığı) hallerde uygulanabilecektir. Buna karşılık adı önceden bilinen ya da doğrudan bulunması hedeflenen bir verinin bulunmadığı, soruşturma konusu suça ilişkin olarak genel olarak bilgisayar içinde delil arandığı hallerde 1. fıkra hükmü uygulanacaktır. Biz çalışmamızda bu arama şeklini ise "bilgisayarda arama" olarak isimlendirdik.

Somut uygulamada "basit arama"nın neredeyse hiç uygulanma imkânı bulunmadığından, biz öncelikle "bilgisayarda arama" kurumunu değerlendirip akabinde "basit arama"yı inceledik.

Bilgisayarlarda yapılacak aramanın hukuki niteliği ve konusu aramanın sınırlarını da belirliyor olduğundan, biz çalışmamızın başında öncelikle bu hususu kısaca tartıştık.

Ayrıca Adli ve Önleme Aramaları Yönetmeliği'nin (AÖAY) 17. maddesinde ve Suç Eşyası Yönetmeliği'nin (SEY) 9/2. maddesinde de bilgisayarda aramaya dönük hükümler bulunduğundan, çalışmamızın ilgili yerlerinde bu maddeleri de değerlendirme konusu yaptık.

Bilgisayarda Aramanın Hukuki Niteliği ve Konusu

Bilgisayarlarda yapılacak arama faaliyetinin hukuki niteliğinin koruma tedbiri olduğu konusunda hiç şüphe bulunmamaktadır. Nitekim bilgisayarda aramanın CMK'da düzenlendiği dördüncü kısmın başlığı da "koruma tedbirleri"dir[1].

---

[1] Koruma tedbirleri teriminin tanımlanmasına ilişkin olarak Türk hukuk doktrinine bakıldığında ortak bir tanımın bulunmadığı görülmektedir. Örneğin; ***Şen "koruma tedbirleri, ceza muhakemesinin gereği gibi sürdürülebilmesi veya hükmün infazının yerine getirilebilmesinin mümkün kılınması amacıyla muhakeme sürecinde başvurulabilen ve hükümden önce, gerektiğinde zor kullanmak suretiyle bazı temel hak ve özgürlüklere geçici müdahaleyi zorunlu kılan uygulamalar" şeklinde tanımlamıştır.*** Bakınız (Bkz.) Ersan Şen – Bilgihan Özdemir, Tutuklama Uygulamada Şüpheli ve Sanık Haklarının Korunması, 3. Bası, Seçkin Yayınevi, Ankara, 2011, s.105.

CMK'nın 134. maddesinin konusu ise,

- Şüphelinin kullandığı bilgisayar,
- Şüphelinin kullandığı bilgisayar programları ve
- Şüphelinin kullandığı bilgisayar kütükleri[2]"dir.

CMK'da her ne kadar "bilgisayar" kavramı kullanılmış ise de, uygulamaya ve doktrine[3] bakıldığında "bilgisayar" kavramı yerine, bilgisayarı da içine alan "bilişim" kavramının kullanıldığı görülmektedir. Nitekim Türk Ceza Kanunu'nda da "bilgisayar" değil "bilişim" kavramı kullanılmıştır (Örneğin 243,244. maddeler). Günümüzde bilgisayar olmamasına rağmen bilgisayarın taşıdığı tüm özellikleri içinde barındıran, ilaveten başka özellikleri de taşıyan (cep telefonu gibi) pek çok cihaz bulunmaktadır. Tek başına "bilgisayar" kavramı bu cihazları kapsayamamaktadır. Bu nedenle kanaatimizce uygulama ve mevzuat birliğini sağlayabilmek ve ayrıca ileride keşfedilecek başka cihazlara da tatbik imkânını sağlayabilmek adına, CMK'da da "bilgisayar" değil "bilişim teknolojileriyle çalışan araçlar" kavramı kullanılmalıdır.

Bu araçlarda aranan delillerin esasında somut varlıkları bulunan şeyler olmayıp, sadece soyut veriler[4] olduğu, bu nedenle elle tutulabilir varlıklarının bulunmadığı unutulmamalıdır.

Bilgisayar Araması

Bilgisayarda Arama

CMK'nın 134. maddesinin 1. fıkrası "*Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine*

Özbek ve arkadaşları *"Ceza muhakemesinin yapılmasını ve bunun sonunda verilecek kararın yerine getirilmesini ve muhakeme giderlerinin karşılanmasını sağlamak için verilen ve hükümden önce temel hak ve özgürlüklere müdahaleyi gerektiren yasal çarelerdir"* şeklinde tanımlamıştır. Bkz. Veli Özer Özbek – M.Nihat Kanbur – Koray Doğan – Pınar Bacaksız – İlker Tepe, Ceza Muhakemesi Hukuku, 2. Bası, Seçkin Yayınevi, Ankara, 2011, s.252.

Şahin ile Öztürk ve arkadaşları da benzer şekilde tanımlar yapmışlardır. Cumhur Şahin, Ceza Muhakemesi Hukuku, 2. Bası, Seçkin Yayınevi, Ankara, 2011, s.197; Bahri Öztürk, Mustafa Ruhan Erdem, Veli Özer Özbek, Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayınevi, 5. Baskı Ankara, 2000, s.553.

[2] Bilgisayar Kütükleri: Bir bilgisayar programı aracılığıyla kullanabilen, verilerin saklandığı genellikle dayanıklı ve uzun ömürlü bir çeşit depolama aracıdır.

[3] Örneğin Fehmi Ünsal Özmestik tarafından hazırlanan ve inceleme konumuzda olan yüksek lisans tezinin başlığı *"Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar"* şeklindedir. Bu tez İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim Ve Teknoloji Hukuku Yüksek Lisans Programı kapsamında 2015 yılında hazırlanmıştır.

[4] "Veri" kavramı (kısaca İnternet Kanunu denilen) 5651 Sayılı Kanun'un 2. maddesinde "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"* şeklinde tanımlanmıştır. AKSSS'de ise veri; ***"bilgisayar sisteminin herhangi bir işlevi gerçekleştirmesine neden olan programı da içermek üzere, olgu, enformasyon ya da kavramların bilgisayar sistemleri içerisinde işlen meye uygun bir biçimde temsili"*** olarak tanımlanmaktadır.

şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir." şeklindedir.

Fıkrada belirtilen unsurları tek tek değerlendirirsek:

- Önceden işlenmiş bir suçun varlığı gerekmektedir.

Madde metninde "*Bir suç dolayısıyla yapılan soruşturmada"* denildiğinden bilgisayar araması yapılabilmesi için mutlaka işlenmiş bir suçun var olması ve bu suç hakkında da soruşturmanın başlamış olması gerekmektedir. Soruşturmanın başlama anı ise, yetkili makamlarca suç şüphesinin öğrenildiği andır (CMK m. 2/1-e).

Bu durumda idari soruşturmalar kapsamında ya da önleyici kolluk faaliyetleri kapsamında bilgisayar araması yapılması mümkün değildir. Kanaatimizce idari soruşturma ve önleyici kolluk faaliyetlerinin çok basit gerekçelerle yapılabilmesi nedeniyle getirilen sınırlama isabetli bir tercih olmuştur. Nitekim bu hususta doktrinde[5] ve uygulamada herhangi bir duraksama da bulunmamaktadır. Örneğin Askeri Yargıtay Daireler Kurulu 22 Ekim 2015 gün ve 2015/89-96 esas ve karar sayılı ilamında[6] bu hususu tartışmış ve bilgisayar aramalarının mutlaka hâkim kararıyla yapılabileceği, disiplin soruşturmaları için bilgisayar araması yapılamayacağı, yapılması halinde ele geçen bilgilerin hukuka aykırı delil olacağı ve hükme esas alınamayacağı vurgulanmıştır.

Türkiye'nin de taraf olduğu Avrupa Konseyi Siber Suçlar Sözleşmesi'nin (AKSSS) bilgisayarda arama ve el koyma işlemlerine yönelik 19. maddesinin gerekçesine baktığımızda da belli bir suç soruşturmasının arandığı görülmektedir. Bu durumda CMK'nın 134/1. maddesinin uluslararası hukuka da uygun olduğu anlaşılmaktadır.

- Suçun işlendiğine dair somut delillere dayanan kuvvetli şüphe sebeplerinin bulunması gerekmektedir.

CMK'da düzenlenen diğer koruma tedbirlerine baktığımızda, koruma tedbirlerine müracaat için kuvvetli şüphenin yeterli kabul edildiğini görmekteyiz. Buna karşılık CMK'nın 134/1. maddesine baktığımızda ise, bilgisayar araması için bu kuvvetli şüphenin yeterli görülmediğini, bu şüphenin somut delillere dayanmasının arandığını görmekteyiz. Bu durumda bilgisayar araması yapılabilmesinin çok zorlaştığı, böylelikle bazı suçluların cezasız kalabileceği akla gelebilir ise de, biz her zaman temel insan

[5] Örneğin bkz. Bülent Yücetürk, "Soruşturmalarda Bilgisayara Elkoyma", Türkiye Bilişim Derneği, Bilişim Dergisi, Yıl:39, Sayı:131, s.103.
[6] Askeri Yargıtay Dairelere Kurulu yine aynı gün verdiği 2015/88-95 esas ve karar sayılı ilamında da benzer görüşü vurgulamıştır.

haklarının öncelikle dikkate alınması gerektiğini düşündüğümüzden, yapılan sınırlandırmayı yerinde görüyoruz. Ancak belirtmeliyiz ki, madde metninde yer alan *"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve"* ibaresi fıkra metninin ilk şeklinde yer almamaktaydı. Bu metin 21 Şubat 2014 tarihli 6526 sayılı kanunun 11. maddesiyle metne eklenmiştir.

Kuvvetli suç şüphesinin ne demek olduğu CMK da açıklanmamıştır. Ancak Centel, Zafer (2008)[7], mevcut deliller ışığında yapılacak bir yargılamada, sanığın mahkûm olmasının kuvvetle muhtemel olması halini kuvvetli suç şüphesi olarak tanımlamaktadır.

Hangi delillerin somut delil olarak kabul edilebileceği ise, her somut olayda ayrı ayrı değerlendirilmelidir. Bu durumda bilgisayarlarda arama kararı veren mahkemenin kararının gerekçesinde "somut delil" olarak neleri kabul ettiğini açıkça belirtmesi gerekmektedir.

CMK'nın 134. maddesi gereği arama yapılacak bilgisayarlar şüphelinin kullandığı bilgisayarlar olmalıdır. Bu durumda bir başka kişinin nezdinde bulunan veya başkasına ait bir bilgisayar ancak şüpheli tarafından kullanmışsa aranabilecektir. Diğer bir deyişle, şüphelinin bulunduğu ortamdaki tüm bilgisayarlar sırf şüpheli tarafından kullanılmış olabilir düşüncesiyle aranamayacaktır.

- Başka suretle delil elde etme imkânının bulunmaması gerekmektedir.

Bu koşul her ne kadar CMK'nın hiçbir maddesinde tanımlanmasa da Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin 4/c maddesinde tanımlanmıştır. Kıyasen de uygulanabilecek bu tanıma göre; *"Soruşturma veya kovuşturma sırasında diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı hususunda bir beklentinin varlığı veya başka yöntemlerden biri veya birkaçının uygulanmasına rağmen delil elde edilememesi ve delillere ancak bu yönetmelikte düzenlenen tedbirlerle ulaşılabilecek olması"* halinde, başka surette delil elde etme imkânının bulunmadığı kabul edilecektir.

Bu durumda başka suretle delil bulma imkânının bulunmaması şartı, bilgisayar aramalarına son çare olarak başvurulması gerektiğini ortaya koymaktadır. Diğer bir deyişle, başkaca bir koruma tedbirinin ya da soruşturma aracının kullanılması yoluyla isnat edilen suç için delil bulunabilecekse, artık bilgisayar araması yapmak mümkün değildir. Ancak burada önemle vurgulamalıyız ki, "başka suretle delil elde etme imkânının bulunmaması" unsuru, diğer koruma tedbirlerine ve soruşturma araçlarına müracaat edilmesine rağmen delil bulunamaması halinde

---

[7] Nur Centel – Hamide Zafer, Ceza Muhakemesi Hukuku; Yenilenmiş ve Gözden Geçirilmiş 5. Bası Beta Yayınları 2008, s 211; Şaban Cankat Taşkın, *"Şüphe Tür ve Dereceleri"*, http://cankattaskin.av.tr/?p=11, E.T. 21.08.2016

otomatik olarak devreye girecek bir unsur değildir. İnsanların özel hayatının gizliliğine ve iletişimine müdahale edilmemesi gerektiğinden, artık delil bulunamadığı zaman bilgisayar araması yapılarak delilin orada bulunabileceğine inanmamızı gerektiren haklı sebeplerin bulunması da gerekmektedir. Nitekim AKSSS'nin gerekçesinin 185. paragrafında bu husus vurgulanarak, bilgisayarda aramanın gerçekleştirilebilmesi için gerekli olan ön koşulun, verilerin belli bir yerde bulunduğuna ve bu verilerin belli bir suça delil teşkil edeceğine inanmak için gerekçelerin var olması olduğu belirtilmiştir.

Açıklanan bu unsurun, kişilerin özgürlüklerini sıkı bir şekilde korumaya alıyor olması nedeniyle kanaatimizce yapılan sınırlama isabetli bir tercih olmuştur.

- Cumhuriyet savcısının istemi üzerine hâkim tarafından karar verilmesi gerekmektedir.

Türk hukuk sisteminde bilgisayar araması yapılabilmesine karar verme yetkisi yalnızca hâkimdedir. Bunun dışında hiçbir şekilde Cumhuriyet savcısının ya da kolluk amirinin yetkisi bulunmamaktadır[8]. Buradaki hâkim soruşturma aşamasında sulh ceza hâkimi, kovuşturma safhasında (yani iddianame kabul edilip duruşmalar başladıktan sonra) ise, yargılamayı yapmakta olan mahkeme hâkimidir[9]. Şayet yargılamayı yapan mahkeme heyet halinde çalışan bir mahkeme ise (örneğin ağır ceza mahkemesi) artık heyetin oy çokluğu ile bilgisayarda arama kararı vermesi gerekmektedir.

---

[8] Yargıtay 19. Ceza Dairesi 06 Mayıs 2015 gün ve 2015/2092 esas ve 2015/1175 karar sayılı kararında CMK'nın 134. maddesi kapsamında mahkemece verilmiş bir bilgisayar araması kararı olmaksızın arama yapılarak suça konu lisanssız yazılımların ve CD'lerin tespit edildiği belirtilerek, bu yazılım ve CD'lerin hukuka aykırı delil olduğu ve hükme esas alınamayacağı belirtilmiştir.

[9] Bu noktada doktrinde kovuşturma evresinde bu koruma tedbirine başvurulamayacağına dair görüşlerinde bulunduğunu belirtmeliyiz.

Bizim düşüncemize göre her ne kadar kovuşturma safhasında da bu karar verilebilecek ise de, sanığın da kararı duruşmada öğrenecek olması nedeniyle, kendisinde bulunan bilgisayar içerisindeki delilleri karartabileceği, böylece arama ile istenen sonuca ulaşılamayacağı şüphesizdir.

Kovuşturma evresinde de CMK'nın 134'üncü maddesinin uygulanabileceğine dair görüşler için bkz. Bahri Öztürk – Durmuş Tezcan - Mustafa Ruhan Erdem – Özge Sırma – Yasemin Saygılar Kırıt – Özdem Özaydın – Esra Alan Akça – Erden Efser, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Ders Kitabı, 6. Baskı, Ankara, 2013, s. 512; Cumhur Şahin, Ceza Muhakemesi Hukuku -I-, 3. Baskı, Ankara 2012, s.250-251; Yusuf Yaşar - İsmail Dursun, "*Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Ve El Koyma Koruma Tedbiri*", Marmara Üniversitesi Hukuk Fakültesi Dergisi, file:///C:/Documents%20and%20Settings/pc/Belgelerim/Downloads/5000001574-5000000750-PB.pdf, E.T. 02/12/2015, s.9; İhsan Baştürk, "*Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma*" Fasikül Dergisi, Ağustos 2010, Sayı:9, s.25.

Yargıtay da kararlarında kovuşturma evresinde bu tedbire başvurulabileceğini kabul etmektedir. Örneğin Yargıtay 1. Ceza Dairesi, 14 Kasım 2005 tarih ve 3891/3230 esas ve karar sayılı kararında bu hususu vurgulamıştır.

Mahkemenin arama karanda mutlaka yazması gereken hususlarsa şunlardır:

- Hangi bilgisayarlarda arama yapılacağı ya da hangi bilgisayara elkonulacağı,
- Hangi suçun soruşturmasıyla ilgili arama yapılacağı,
- Aramanın yapılacağı tarih ve zamanın ne olduğu,
- Aramaya sebep olan şüphenin nasıl oluştuğu,
- Arama için bilgisayara neden başvurulmak zorunda olunduğu,
- Elde edilecek olan dijital delil niteliğindeki verilerin nasıl koruma altına alınacağı ve
- Bu elde edilecek delillerin başka soruşturmalar için kullanılıp kullanılmayacağı hususlarının kararda bulunması, ileride yapılması muhtemel birçok (hukuksal) tartışmayı daha baştan engellemiş olacaktır.

- Aramanın konusunun sadece şüphelinin kullandığı bilgisayar, bilgisayar programı veya bilgisayar kütüğü olması gerekmektedir.

Madde metninde bu araçları şüphelinin kullanması arandığından, söz konusu araçların kime ait olduğunun önemi bulunmamaktadır. Kanaatimizce, aramaya konu olacak araç bizzat şüpheliye ait değilse, yapılacak arama için aracın sahibinin ya da temsilcisinin de hazır bulunmasına imkân sağlanmalıdır. Çünkü aracın sahibi olan şahsın özel hayatına ilişkin veriler bu araçların içerisinde bulunmaktadır ve yapılacak aramayla bunlar başkaları tarafından öğrenilecektir.

Şüphelinin kullanmadığı bilgisayar, bilgisayar programları veya bilgisayar kütükleriyse sırf şüpheliyle aynı mekânda bulunduklarından bahisle aranamayacaktır. Örneğin şüphelinin iş yerinde bulunan bütün bilgisayarlar değil, sadece şüphelinin kullandığı bilgisayar aranmalı ve şüphelinin kullandığına dair açık delil bulunmadıkça sırf şüphelinin de kullanmış olabileceği ihtimaliyle, yan masada dahi olsa, diğer bilgisayara dokunulmamalıdır.

Görüldüğü üzere bilgisayar aramasının yapılabileceği araçlar sınırlı şekilde sayılmıştır. Bunların dışındaki araçlarda artık CMK'nın 134. maddesinin uygulanması mümkün değildir. Ancak günümüzde internetin yaygınlığı ve insanların artık pek çok bilgisini ve verisini kişisel bilgisayar ortamında değil de, internet ortamında tuttuğu dikkate alındığında, bilgisayar ağı üzerinden başka araçlarda (örneğin bulut) arama yapılmasının mümkün olup olamayacağını tartışmamız gerekmektedir.

CMK'nın 134. maddesine baktığımızda uzaktan erişimle arama yapılabileceğine dair bir hükmün bulunmadığı görülmektedir. Ancak bu noktada AÖAY'nin 17. maddesinin 3. fıkrasına baktığımızda *"Bilgisayar veya bilgisayar kütüklerine elkonma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır*" denilmek suretiyle CMK'da düzenlenmeyen

araçlarda da aramaya imkân verildiğini görmekteyiz. Diğer bir deyişle, CMK'da bulunmayan iç ağ veya internet üzerinden bağlanılan, başka bir fiziki mekânda bulunan, sunucu veya bilgisayar sistemi unsurlarında da aramaya yönetmelikle imkân tanınmıştır[10]. Ancak yönetmelik hükümlerinin kanunlara aykırı olamayacağına ilişkin normlar hiyerarşi kuralını dikkate aldığımızda, şüpheli aleyhine bilgisayar aramasını genişleten bu yönetmelik hükmünün hukuka aykırı olduğunu belirtmemiz gerekmektedir. Bu çelişkiye rağmen belirtmeliyiz ki, özellikle internetin sağladığı kolaylıklar ve delillerin internet ortamında saklanabileceği milyonlarca alan dikkate alındığında, kanaatimizce mutlaka CMK kapsamında da ağ üzerinden aramaya imkân sağlanması gerekmektedir. Ancak bu noktada uzaktan erişimin yaratacağı sorunların giderilebilmesi için kanaatimizce, arama öncesinde mutlaka fail ya da vekili arama sırasında hazır bulundurulmalı, vekili yoksa zorunlu müdafii atamasının yapılması, ayrıca mümkünse arama yapılacak failin kullanımına tahsis edilen kısmın imajının alınması ve aramanın artık imaj üzerinden yapılması, failin kullanımına tahsis edilmeyen alanlara kesinlikle girilmemesi, ayrıca ağ üzerinden erişilen alanın suçla ilgili olmadığı anlaşıldığında derhal oradan çıkılması, tüm bu faaliyetler sırasında orantılılık prensibinin uygulanması gerekmektedir.

Bu noktada vurgulanması gereken bir husus ise, günümüzde yaygın olarak kullanılan sanallaştırma teknolojilerinin, geleneksel fiziksel depolama ortamlarından farklı olarak, her müdahale ya da imaj alma işlemi sırasında farklı hash değeri verebileceğidir. Bu nedenle bir kez kopya alındıktan sonra sistem üzerinden yeniden kopya almak yerine, alınan kopyanın bir kopyası daha çıkartılarak taraflara verilmesi gerekmektedir. Aksi durumda taraflarda bulunan kopyaların hash değerleri farklı olacağından, artık kopyaların delil değeri de tartışmalı hale gelecektir.

Bu kapsamda AKSSS'ne baktığımızda, sözleşmenin gerekçesinin 187 nolu paragrafında uzaktan erişimin önemine *"…ulusal mevzuatların uzaktan aramaları da mümkün kılacak şekilde düzenlenmesi, bu anlamda uluslararası işbirliği bakımından da buna mevzuatta yer verilmesi son derece önemlidir"* şeklinde ifadeye yer verildiğini, ancak erişimin nasıl yapılması gerektiği hususunun açıklanmadığını görmekteyiz.

CMK'nın 134. maddesiyle AÖAY'nin 17. maddesi birlikte değerlendirildiğinde, kanaatimizce CMK'nın 134. maddesinde geçen *"bilgisayar, bilgisayar programları ve bilgisayar kütüklerinde arama"* ifadesi yerine, "*bilişim sistemlerinde ve veri saklama araçlarında arama ve elkonma*" şeklinde ifadenin kullanılması çok daha yerinde olacaktır. Böylelikle verinin saklandığı yerlerin tamamıyla, nakledildiği yerlerin tamamı aramaya konu olabilecektir.

[10] Fatih Berber, "*Bilgisayar Kütüğü Ne Demektir?",* http://fatihberber.com/tag/bilgisayar-kutugu/ E.T. 20/12/2015

Yönetmelikte yer alan "çıkarılabilir donanımlar" ifadesiyle CD, harici bellek (flash disk) gibi aygıtlar ifade edilmektedir. Bunlar esasında bilgisayar kütüğü olarak kabul edilebileceğinden, kanaatimizce CMK'nın 134. maddesi kapsamında kalmaktadır.

Bilgisayarda arama konusunda tartışılabilecek bir diğer husus, CMK'da düzenlenmese de, mağdura ait bilgisayarda mağdurun rızasıyla arama yapılıp yapılamayacağıdır. Kanaatimizce, mağdurun bilgisayarında yapılan aramayla da sanık aleyhine delil toplanmaktadır. Dijital delillerin kolaylıkla değiştirilebilir ve sahtesinin yapılabilir olunduğu dikkate alındığında, elde edilen delillerin gerçekliği her zaman şüpheli kalacaktır. Bu nedenle mağdurun rızası varsa artık her ne kadar mahkeme kararı gerekmeksizin arama yapılabilecekse de, bu arama öncesinde de ilk olarak imaj alımının yapılması, aramanın da bu imaj üzerinden yapılması, böylelikle delil bütünlüğünün korunması gerektiğini düşünmekteyiz. Çünkü pekâlâ mağdurun kendi kendine sanık adına gönderdiği verilerle iftirada bulunması da mümkündür.

CMK'nın 134. maddesinde cep telefonuna yer verilmemesi nedeniyle cep telefonlarında arama yapılmasının mümkün olup olmadığı da tartışılmalıdır. Kanaatimizce cep telefonunda arama yapılması gerekirse öncelikle cep telefonunun bilgisayar özelliğinin olup olmadığına, internete erişim imkânının olup olmadığına bakılmalıdır. Bu soruların cevabının hayır olması halinde artık CMK'nın 134. maddesi uygulanamayacaktır. Bu sorulardan birinin cevabının evet olması halinde ise, söz konusu cep telefonu bilgisayar ya da en azından bilgisayar kütüğü olarak kabul edileceğinden, bu telefonda CMK'nın 134. maddesi kapsamında arama yapılması mümkün olacaktır. Ancak önemle vurgulayalım ki, cep telefonunda yapılacak arama da amaç bilgisayar ortamında saklanabilecek bir delile ulaşmak değil de, iletişimin tespitine ilişkin delillere ulaşmaksa, CMK'da iletişimin tespiti konusu özel olarak düzenlendiğinden, artık bilgisayar araması yapılamayacaktır. Kaldı ki, bilgisayar aramasının son çare olduğu, daha önce başka yollarla delil elde etme imkânının bulunduğu durumlarda bu yola başvurulamayacağı dikkate alındığında da bilgisayar araması yapılamayacağı (öncelikle iletişimin tespiti yoluna gidilmesinin gerekeceği) sonucuna ulaşılmaktadır.

Bilgisayar aramasını değerlendirirken açıklanması gereken bir diğer husus da, bu aramayı kimin yapacağıdır. CMK ve diğer mevzuatta dijital delillerin kimler tarafından toplanacağına ilişkin doğrudan bir hüküm bulunmamaktadır. Ancak, CMK'nın 160/2. maddesi gereğince, Cumhuriyet savcısının emrindeki adli kolluk görevlileri vasıtasıyla, şüphelinin lehinde ve aleyhinde olan tüm delilleri toplaması gerekmektedir. Bu durumda savcılık makamının bilgisayar ve her türlü çevre biriminden elektronik delile ulaşma imkânı bulunmaktadır. Ancak unutulmamalıdır ki, elektronik delil, tıpkı parmak izi veya DNA gibi, ilk başta gözle görülemeyen gizli bir yapıya sahiptir ve rahatlıkla tahrip veya yok edilebilir;

ayrıca, zamana karşı da son derece hassastır[11]. Bu durumda söz konusu araçlarda yapılacak aramanın özel uzmanlık gerektiriyor olması nedeniyle, kanaatimizce adli kolluğun uzman birimlerince ya da atanacak uzman bilirkişilerce delillerin toplanması yapılmalıdır. Kanaatimizce ileride yaşanacak delillerin gerçekliği tartışmalarının önüne geçilebilmesi için savcının bizzat aramaya eşlik etmesi de faydalı olacaktır.

Bilgisayarda Basit Arama

CMK'nın 134/5. maddesi *"Bilgisayar veya bilgisayar kütüklerine elkonmaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır"* şeklindedir.

CMK'nın 134. maddesinin 5. fıkrasında düzenlenen arama işlemine "basit arama" diyebiliriz. Çünkü bu arama önceden bilinen belirli bir unsurun arandığı hallerde (örneğin adı belli bir dosyanın arandığı hallerde) uygulanabilecek olan arama olup, bu aramanın yapılması halinde kopyası alınan verilerin mutlaka ama mutlaka kâğıda yazdırılması ve bu durumun tutanakla da tespit edilerek ilgililere imzalatılması gerekmektedir.

Basit arama işleminin unsurlarını tek tek değerlendirirsek:

- Arama bilgisayar veya bilgisayar kütüklerinde yapılmalıdır.

Önceki fıkralarda bilgisayar programları da aramaya konu yapılmışken, burada yapılmaması kanaatimizce isabetli bir tercih olmuştur. Çünkü sistemin çalışması ya da sistemde belli bir görevin yapılabilmesi için hazırlanan bilgisayar programlarının incelenmesi, çıktı alınan kâğıt üzerinden değil, sadece sistem üzerinde yapılabilecektir.

Bilgisayar ve bilgisayar kütükleri hakkında yukarıda yaptığımız açıklamalar burada da geçerlidir.

- Arama sonunda verilerin tamamının veya bir kısmının kopyası alınmalıdır.

Aşağıda elkonma tedbirini değerlendirirken ayrıntılarıyla tartışacağımızdan dolayı, burada bu unsuru tartışmayacağız. Ancak belirtmeliyiz ki, delil güvenliği ve güvenilirliğini sağlamak için, yedeklemenin imaj alım ve hash değeri belirlenmek suretiyle yapılması çok daha faydalı olacaktır.

- Kopyası alınan veriler kâğıda yazdırılmalı ve bu durum bir tutanağa da bağlanarak ilgililer tarafından imzalanmalıdır.

[11] Amerika Birleşik Devletleri Adalet Bakanlığı Ulusal Adalet Enstitüsü (U.S. Department of Justice National Institute of Justice) (2001), "*Electronic Crime Scene Investigation: A Guide For First Responders*", http://www.ncjrs.gov/pdffiles1/nij/187736.pdf, s.6.

Bu şart inceleme konusu aramayı uygulanamaz hale getirmiştir. Çünkü en basit bilgisayar delilinde dahi bazen binlerce hatta milyonlarca sayfa çıktı kâğıt alınması gerekecektir. Bu kadar çok belgenin incelenmesi bir yana, nakli ya da belli bir yerde korunması dahi çok zor olmaktadır. Örneğin delil olan bir sayfanın aradan alınmasını kimse fark edemeyecektir. Kanaatimizce elektronik ortamda bulunan delillerin incelenmesi de elektronik ortamda olmalıdır. Bu inceleme sırasında sadece ihtiyaç duyulan sayfaların çıktısının alınarak bu kısımların kâğıt üzerinden incelemesi ise zaten mümkündür.

Kanaatimizce bilgisayarda basit arama kurumunun tatbikinin imkânsızlığı ve delil güvenliğini, güvenilirliğini sağlamıyor olması nedeniyle CMK'dan tamamen kaldırılması gerekmektedir. Bu kapsamda yapılacak aramaların 1. fıkra kapsamında ve çok daha güvenle yapılabileceği unutulmamalıdır.

Bilgisayar Ortamında Elkonma

CMK'nın 134. maddesinin 2. fıkrası "*Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir*" şeklindedir.

CMK'nın 134. maddesinin 2. fıkrasındaki elkonmanın nasıl yapılacağı hususu ise, 3. fıkrada "*Bilgisayar veya bilgisayar kütüklerine elkonma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır*" şeklinde ve 4. fıkrada *"Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır"* şeklinde düzenlenmiştir.

Görüldüğü üzere sistem içerisinde gizlenmiş veri niteliğinde delillerin bulunduğu düşünülüyor ve bunlara hemen orada ulaşılamıyorsa ya da bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilemiyorsa artık delillere ulaşılabilmesi için, bu fıkra gereğince elkonma işleminin yapılması gerekmektedir.

Elkonma işleminin unsurlarını tek tek değerlendirirsek:

- Elkonmaya konu olabilecek araçlar bilgisayar, bilgisayar programları ya da bilgisayar kütüğüdür.

Bu araçlara ilişkin olarak yukarıda yaptığımız açıklamalar burada da geçerlidir.

- Elkonulabilmesi için şifresinin çözülememesi ya da gizlenmiş bilgilere ulaşılamamış olunması gerekmektedir. Diğer bir deyişle, elkonmanın, çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi amacıyla yapılması gerekmektedir.

Bilgisayar araması kararından sonra, yapılacak arama sırasında, inceleme konusu aracın şifreli olmasından dolayı sisteme girilememesi ya da sisteme girilmesine rağmen sistem içinde gizlendiği düşünülen bilgilere ulaşılamaması halinde elkonma yapılabilecektir. Bu durumda sistemin şifreli olmaması halinde ya da gizlenmiş bir verinin bulunmadığının düşünülmesi halinde elkonma işlemi yapılamayacaktır.

Görüldüğü üzere arama işlemine konu olmamış araçların, doğrudan elkonma işlemine konu edilmesi mümkün değildir. Zira veriye ulaşılabilmesi için her şeyden önce arama yapılması gerekmektedir.

Kanaatimizce bu koşul yeniden kaleme alınmalı ve arama yapılacak bilgisayara hiçbir işlem yapılmadan (aşağıdaki diğer şartlarında bulunması şartıyla) doğrudan elkonma tedbirinin uygulanması imkânı sağlanmalıdır[12]. Çünkü,

- Arama için bilgisayara müdahale edilmesi halinde, en basit hareketle kapalı sistemin açılması halinde dahi bilgisayarda bulunan koruyucu programlar sayesinde delillerin yok edilmesi mümkündür.
- Gizlenmiş bir delilin olup olmadığının tespitinin hangi kıstaslarla yapılacağı belli değildir. Bu durumda saatlerce hatta günlerce şüphelinin evinde, iş yerinde ya da aleni bir alanda ve hatta tehlikeli bir alanda aramaya devam edilmesi gerekebilecektir. Oysaki hiç kimse ne evinde ne işyerinde ne de aleni alanlarda kolluk görevlilerini bu kadar süreyle görmek istemeyecektir. Nitekim uygulamaya bakıldığında da, kanunda aranan şartlar gereği değil, aramanın uzun süre alacak olması nedeniyle, doğrudan imaj alımına gidildiği görülmektedir.

- Şifrenin çözülmesi ve gerekli kopyanın alınması halinde elkonulan araçların gecikme olmaksızın iadesi gerekmektedir.

Bu yönüyle de CMK'nın 134. maddesinin mutlaka değiştirilmesi gerekmektedir. Çünkü iade konusunda maddede hiçbir ayrım yapılmaksızın iade şart koşulmuştur. Ancak toplum menfaatleri ve 3. şahısların çıkarları dikkate alındığında sınırsız bir şekilde iade kabul edilemez. Örneğin, elkonmaya konu yapılan delilin, devlet sırrı, çocuk pornosu gibi bizzat bulundurulması yasak olan bir veri olması da mümkündür. Böylesi hallerde elde bulunan bu verilerin şüpheli ya da vekiline verilmemesi gerekecektir. Diğer bir deyişle, delilin bulundurulmasının suç teşkil ettiği hallerde şüpheli ya da vekiline anılan kayıtların verilemeyeceği kanunda açıkça düzenlenmelidir. Bu durumda ileride delillerin değiştirildiği iddiasıyla karşılaşılmaması için, alınan imajların şüpheli ya da vekiline verilmesi gereken suretinin kapalı ve mühürlü zarfla (yargılama kesin hükümle bitinceye kadar) adli emanette muhafazası sağlanmalıdır. Ayrıca saklanan verilerin hash değeri şüpheli ya da vekiline tutanakla verilmelidir. Bu

---

[12] Benzer açıklama için bkz. Yunus Balı, "*CMK 134 Düzeltilmelidir*", http://www.dijitaldeliller.com/cmk134.htm, 15/05/2016.

noktada önemle belirtelim ki, savunma hakkının dokunulmazlığı dikkate alındığında şüpheli ya da vekilinin bu delilleri incelemek istemesi halinde, engel olunmaksızın incelemelerine imkân sağlanmalıdır.

Ayrıca belirtelim ki, böylesi durumlarda Türk Ceza Kanunu'nun müsadereye ilişkin hükümlerinden faydalanmak da mümkündür.

- Elkonma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılmalıdır.

Bu yedekleme işlemine uygulamada imaj alma işlemi denilmektedir[13]. İmaj almanın ve aramanın da bu imaj üzerinden yapmanın önemi hash değerinin alınmasından kaynaklanmaktadır. Hash değeri yedeklenen bilişim aracının parmak izi niteliğindedir. Hash değerine elektronik mühür de denilmektedir**.** Yedeklenen verilerin bir noktasının dahi değiştirilmesi halinde hash değeri değişeceğinden, imaj almakla yedeklenen verilerin yani delillerin güvenliği ve güvenilirliği de sağlanmaktadır. Kolluktaki ve şüpheli ya da vekilindeki imajın hash değerlerinin birbirini tutmaması halinde, imaj üzerinde değişiklik yapıldığı anlaşılacağından, artık o kayıtların sanık aleyhine delil olarak kullanılması mümkün olamayacaktır.

Bu noktada unutulmaması gereken husus, hash değerlerinin birbirini tutması her ne kadar delillerin değiştirilmediğini ortaya koymakta ise de, bu delil değeri yalnızca şekli anlamdadır. Yani, pekâlâ imaj alımı öncesinde 3. kişiler tarafından zararlı yazılımlarla ya da doğrudan müdahaleyle şüphelinin bilgisayarına uydurma delillerde konulmuş olunabilecektir. Bu nedenle, elde edildiği iddia edilen delillerin sanıkla bağının ve bu delillerin gerçekliğinin ayrıca araştırılması gerekmektedir.

Yedekleme işlemi, elkonma öncesinde veya sırasında yapılmalıdır. Diğer bir deyişle, söz konusu araçların başka bir yere nakli elkonma işleminden sonra mümkündür. Elkonma işleminden sonra yapılacak yedekleme işlemi, verilerin güvenliği açısından sakınca yaratacaktır. Aksi durum, elde edilen delillerin hukuka aykırı delil olmasına da yol açacaktır. Konuyu vurgulayan Yargıtay 11.Ceza Dairesi 16 Nisan 2007 tarih 2005/6376 esas ve 2007/2551 karar sayılı kararında *"... söz konusu dosyanın birebir (sector-by-sector) yedeğinin alınması (yani incelemenin orijinal dosya üzerinde yapılmaması), daha sonra ikinci olarak alınan birebir yedeğin değiştirilip değiştirilmediğini tespite yarayacak zaman ve bütünlük kontrolü imkânı sağlayan değerin (hash) belirlenmesi, ... gerektiği hususları da göz önüne alınarak ... ve toplanan deliller bir bütün halinde değerlendirildikten sonra sonucuna göre sanığın hukuki durumunun takdir ve tayini gerektiği gözetilmeden eksik inceleme ile ..."* şeklinde karar vermek

[13] Yargıtay 8. Ceza Dairesi 24 Ekim 2013 gün ve 2012/21817 esas ve 2013/25248 karar sayılı kararında imaj alımının usulüne uygun yapılmadığı belirtilerek şüpheden sanık yararlanır ilkesine ulaşıp sanığın beraatine karar verilmesi gerektiğini belirtmiştir.

suretiyle incelemenin mutlaka hash değeri tespit olunan elkonulan yedek kopya üzerinden yapılması gerektiğini vurgulamıştır.

Yedekleme yapılırken sistemin bir kısmının değil tamamının imajının alınması gerekmektedir. Böylelikle silinmiş dosyaların dahi yedeklemesi yapılmış olunacaktır.

Kanaatimizce bu koşul, delil bütünlüğünün sağlanması ve sistemde değişiklik yapıldı iddiasıyla karşılaşılmaması bakımından isabetli bir düzenlemedir. Ancak uygulama açısından tatbiki zor bir şarttır. Çünkü basit bir eve gidildiğinde dahi, bilgisayar kütüğü niteliğinde onlarca cd, dvd, harici bellek bulunabilecektir. CMK'nın 134. maddesine baktığımızda bunların tamamının yedeklenmesi gerekmektedir. Bu durumda inanılmaz bir zaman harcanması söz konusu olacağı gibi, bunların incelenmesindeki güçlüklerde reddedilemez. Özellikle örgütlü suçlarda ele geçebilecek CD, DVD sayısının bile binlerce olacağı dikkate alındığında imkânsızlık çok daha açık bir şekilde karşımıza çıkmaktadır. Örneğin görünüşte bir film DVD'si olarak gözüken ve ilk bakışta da film şeklinde başlayıp, devam edip biten bir DVD'nin 67. dakikasına suça ilişkin bir delilin konulması mümkündür. Bu durumda filmin tamamını seyretmedikçe bu delil bulunamayacaktır.

- Alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmesi ve ayrıca bu verme işleminin de tutanağa geçirilerek imza altına alınması gerekmektedir.

CMK'nın 134/4. maddesi *"istemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır"* şeklinde iken 21 Şubat 2014 tarihli ve 6526 sayılı Kanunun 11. maddesiyle "*İstemesi halinde, bu*" ibaresi "*Üçüncü fıkraya göre alınan*" şeklinde değiştirilmiştir. Bu durumda imaj alımı yapıldıktan sonra mutlak surette bir yedeğin çıkartılması ve şüpheliye ya da vekiline verilmesi gerekmektedir. Görüldüğü üzere kanun koyucu, isteği olup olmadığına bakılmaksızın bilişim cihazından çıkarılan yedekten bir kopyanın, bilişim cihazını kullanan şüpheli veya vekiline teslimini emretmiştir. Kanaatimizce delil güvenliğini ve güvenilirliğini sağlaması nedeniyle yapılan değişiklik yerinde bir değişiklik olmuştur.

Burada şüpheliye ya da vekiline verilmesi gereken yedek, kolluk kuvvetlerince alınan imajın yedeği olmalıdır. Diğer bir deyişle, aramaya konu araçtan yeniden imaj almak yerine alınan imajın kopyası çıkarılmalı ve şüpheli ya da vekiline verilmelidir. Bu safhadan sonra yapılacak aramalar artık aramaya konu araç üzerinde değil, alınan imaj üzerinden olmalıdır.

Bir kopyanın şüpheli veya vekili tarafından herhangi bir nedenle alınmak istenmemesi halinde ne olacaktır. Kanaatimizce elkonmayı yapan kişilerce durum bir tutanakla tespit edilip, akabinde bu tutanak yedeklenen veriyi almaktan kaçınan şüpheli veya vekiline de imzalatılmalıdır. Şüpheli ya da vekilinin tutanağı imzalamaktan da kaçınması halinde, tutanağa bu husus da yazılmalıdır.

Akabinde şüpheli ya da vekilinin almadığı yedek kopya bir zarf ya da torbaya konulmalı ve şüpheli veya vekilinin alabileceği şekilde adli emanete konulmalıdır. Aksi takdirde bilişim cihazlarına elkonulması suretiyle yapılan aramalarla ilgili sahtelik iddialarının önünü alabilmek mümkün olamayacaktır[14].

Bu noktada vurgulamalıyız ki, uygulamada sıklıkla depolama yapılacak araçların kim tarafından temin edileceği, bedelini kimin ödeyeceği sorunu yaşanmaktadır. Kanaatimizce, yedekleme yapılacak depolama araçları Cumhuriyet savcılığınca temin edilmelidir. Yargılama sonunda failin mahkûm olması halinde depolama araçlarının bedeli, yargılama gideri kapsamında, failden alınabilecektir. Failin beraat etmesi halinde ise, artık bedel devlet hazinesinden karşılanacaktır.

Ekonmayı açıklarken Suç Eşyası Yönetmeliği'nin 9/2. maddesine de[15] değinmemiz gerekmektedir. Burada el konulan verilerin nasıl korunacağı hususu düzenlenmiştir. Fıkra metni *"...Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir…"* şeklindedir. Bilgisayara ilişkin delillerin ve özellikle de imaj muhafaza edilen araçların manyetik alanlardan ve nem gibi iklimsel koşullardan kolaylıkla etkilenebileceği dikkate alındığında yapılan düzenleme yerinde bir düzenlemedir. Bu dijital delillerin gerek fiziki gerekse manyetik olarak mutlaka korunması gerekmektedir.

Sonuç

Sonuç olarak görülüyor ki, CMK'nın 134. maddesinde düzenlenen arama ve elkonma, kişilerin hak ve özgürlüklerini yakından ilgilendirdiğinden mutlaka kanunda bulunması gereken bir hükümdür. Ancak insan hakları ihlallerine sebep olabilecek yapıda olması nedeniyle CMK'nın 134. maddesi başlığıyla birlikte yeniden düzenlenmelidir. Bu kapsamda mevcut metne ilişkin değişiklik gerekçelerimizi şu şekilde sıralayabiliriz:

- Günümüz teknolojisi dikkate alındığında "bilgisayar" kavramının ihtiyacı karşılamaması; ayrıca uygulamada ve Türk Ceza Kanunu'nda da "bilgisayar" değil "bilişim" kavramının kullanılması nedeniyle (yani kavram birliğinin de sağlanabilmesi amacıyla) madde başlığı ve metninde "bilişim" kavramı kullanılmalıdır.

---

[14] Benzer açıklamalar için bkz. Ersan Şen, "*Bilgisayar Verilerinin Yedeklenmesi ve Yasak Veriler"*, http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1182294-bilgisayar-verilerinin-yedeklenmesi-ve-yasak-veril E.T. 10.12.2015.

[15] Söz konusu maddenin başlığı *"Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler"* şeklinde olup, içeriğinde ise, 2. fıkra dışındaki fıkralar bilgisayarlara dönük değildir.

- Kanunda düzenlenmeyen uzaktan erişimle ve hatta çevrim içi erişimle[16] delil toplama imkânı mutlaka getirilmeli, ancak bu durum çok sıkı şartlara bağlanarak sanığın ya da 3. şahısların özel hayatlarının ifşasına engel olunmalı, başka devletlerin egemenlik haklarına saygı duyulmalıdır.
- CMK'nın 134/5. maddesinde yer alan (ve bizimde çalışmamızda "Bilgisayarda Basit Arama" başlığı altında incelediğimiz) metnin, neredeyse hiç uygulanma kabiliyeti bulunmayan bir metin olması nedeniyle; uygulandığında ise, delil güvenliği ve güvenilirliğini sağlamaması nedeniyle ve ayrıca bu kapsamda yapılabilecek aramaların zaten 1. fıkra kapsamında da yapılabilecek aramalar olmaları nedeniyle tamamen yürürlükten kaldırılmalıdır.
- Mevcut metne göre sistemin şifreli olmaması halinde ya da gizlenmiş bir verinin bulunmadığının düşünülmesi halinde elkonma işlemi yapılamayacaktır. Oysaki delillerin sağlıklı bir şekilde ele geçirilebilmesi ve bütünlüğünün korunabilmesi için daha aramaya başlamadan önce elkonulması ve elkonulan veriler üzerinden aramanın yapılması gerekmektedir. Bu nedenle elkonma şartlarının da yeni baştan düzenlenmesi gerektiğini düşünmekteyiz.
- Mevcut metne göre elkonulan verilerin derhal sahibine iadesi gerekmektedir. Kanaatimizce, bu cümle de yeniden yazılmalı ve elkonulan verilerin bizzat bulundurulmasının dahi suç olduğu hallerde sahibine iadesinin önüne geçilmelidir.

Ayrıca belirtmeliyiz ki, bilgisayar ortamında kolaylıkla sahte veriler üretilebilmesi ya da mevcut verilerde kolaylıkla değişiklik yapılabilmesi nedeniyle, tek başına bu delillere güvenilerek mahkûmiyet hükmü kurulmamalıdır. Mutlaka bu delillerin başka delillerle de desteklenip desteklenmediği araştırılmalıdır. Başka delillerle desteklenmediği sürece şüpheden sanık yararlanır ilkesi dikkate alınmalıdır.

Son olarak belirtelim ki, CMK'nın ***134. maddesine aykırı olarak bilgisayarlarda arama veya elkonma işlemi yapılmışsa, elde edilen deliller artık hukuka aykırı deliller olacağından hükme esas alınamayacaklardır.***

Kaynakça

Amerika Birleşik Devletleri Adalet Bakanlığı Ulusal Adalet Enstitüsü (U.S. Department of Justice National Institute of Justice), (2001). *Electronic Crime Scene Investigation: A Guide For First Responders*, http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

[16] Çevrimiçi arama, devlet soruşturma makamları tarafından üçüncü kişilere ait bilişim sistemleri üzerinde iletişim araçlarını kullanarak gizlice icra edilen erişim olarak tanımlanmaktadır. Cengiz Tanrıkulu, "*Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama Ve Elkoyma"*, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Doktora Tezi, Ankara, 2014, s. 280.

BALI, Y., CMK 134 Düzeltilmelidir, http://www.dijitaldeliller.com/cmk134.htm, E.T. 15/05/2017.

BAŞTÜRK, İ., (2010). Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma. *Fasikül Dergisi.* Sayı:9.

BERBER, F., Bilgisayar Kütüğü Ne Demektir?, http://fatihberber.com/tag/ bilgisayar-kutugu/

CENTEL, N., **ZAFER,** H., (2008). *Ceza Muhakemesi Hukuku*, İstanbul: Beta.

TAŞKIN, Ş.C., Şüphe Tür ve Dereceleri. http://cankattaskin.av.tr/?p=11

ÖZBEK, V.Ö., **KANBUR,** M.N., **DOĞAN,** K., **BACAKSIZ** P., **TEPE,** İ. (2011). *Ceza Muhakemesi Hukuku.* Ankara:Seçkin.

ÖZMESTİK F.Ü., (2015). *Bilişim Sistemleri Üzerine Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar.* Yayınlanmamış Yüksek Lisans Tezi. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü

ÖZTÜRK, B., **ERDEM** M.R., **ÖZBEK,** V.Ö., (2000). *Uygulamalı Ceza Muhakemesi Hukuku*, Ankara:Seçkin.

ÖZTÜRK, B., **TEZCAN** D., **ERDEM,** M.R., **SIRMA** Ö., **KIRIT,** Y.S., **ÖZAYDIN,** Ö., **AKÇA,** E.A., **EFSER** E., (2013). *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, Ankara: Seçkin.

ŞAHİN, C. (2011). *Ceza Muhakemesi Hukuku*, Ankara: Seçkin.

ŞEN, E., Bilgisayar Verilerinin Yedeklenmesi ve Yasak Veriler. http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1182294-bilgisayar-verilerinin-yedeklenmesi-ve-yasak-veril

ŞEN, E., **ÖZDEMİR,** B., (2011). *Tutuklama Uygulamada Şüpheli ve Sanık Haklarının Korunması*, Ankara:Seçkin.

TANRIKULU, C., *Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama Ve Elkoyma*, Yayınlanmamış Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

YAŞAR Y., **DURSUN,** İ., Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Ve El Koyma Koruma Tedbiri. *Marmara Üniversitesi Hukuk Fakültesi Dergisi*, file:///C:/Documents%20and%20Settings/pc/Belgelerim/Downloads/5000001574-5000000750-PB.pdf.

YÜCETÜRK, B., Soruşturmalarda Bilgisayara Elkoyma. *Türkiye Bilişim Derneği Bilişim Dergisi*, Yıl:39, Sayı:131.

Unutulma Hakkı: Dijitalleşme Sürecinde Bilgiye Erişim Özgürlüğünü Tehdit Eder mi?

Yrd. Doç. Dr. Halise ŞEREFOĞLU HENKOĞLU

Adnan Menderes Üniversitesi Yönetim Bilişim Sistemleri Bölümü

Özet

Dünya çapında milyonlarca kullanıcıya hizmet veren ve küresel olarak bilgiye erişim ve iletişim aracı olarak kullanılan internet, bireysel ve kurumsal boyutta temel hak ve özgürlüklerin kullanımında sağladığı avantajlarının yanı sıra, ilgili hak ve özgürlüklerin kullanımında farklı boyutları da beraberinde getirmektedir. 1990'lı yıllarda birçok fütürist tarafından dünyayı yeniden şekillendireceği ve yeni bir dünya düzeni yaratacağı öngörülen internet, bugün bilgiye erişimde sunduğu sınırsız imkânlar ile birlikte yeni bir tartışmanın da fitilini ateşlemektedir. Kişisel verilerin ve dijital mahremiyetin korunması, bilgi edinme hakkı, bilgiye erişim özgürlüğün sağlanması olgularının dengesi üzerinde şekillenen bu tartışmanın temelinin ise, "unutulma hakkı" kavramına dayandığını söylemek mümkündür. Son zamanlarda kişisel verilerin korunmasına ilişkin başlıklar ile gündeme gelen unutulma hakkı (right to be forgotten/oblivion), uluslararası hukukta oldukça tartışmalı ve eleştiriye açık bir konu olarak dikkat çekmektedir. Genel bir bakış açısıyla ele alındığında, unutulma hakkını; "bireyin dijital ortamda yer alan kişisel verilerinin çeşitli sebeplere bağlı olarak silinmesini ve daha fazla yayılmasının önlenmesini talep etme hakkı" olarak tanımlamak mümkündür. Kendisi de sınırsız dijital bir arşiv olan internet ortamının yanı sıra, özel veya devlete bağlı kurum ve kuruluşlar tarafından oluşturulan dijital arşivlerde de saklanan kişisel verilerin korunması ile yakından ilişkili olan bu hak, birçok ülkede yasal düzenlemeler ile korunmaktadır. 13 Mayıs 2014 tarihinde Avrupa Adalet Divanı tarafından yasal hale getirilen unutulma hakkı, ilk bakışta kişilerin sahip olması gereken temel hak ve özgürlükler kapsamında dijital mahremiyetin korunmasına yönelik olumlu bir adım olarak görülse de, kişilerin bilgiye erişim özgürlüğüne zarar vereceği ve dijital ortamda iletişim ve ifade özgürlüğünü engelleyeceği de sıkça dile getirilmektedir. Avrupa Birliği ülkelerinde yasal düzenlemeler ile sınırları kesin bir şekilde çizilen unutulma hakkı, kapsamı ve uygulanma süreci açısından uluslararası boyutta farklı şekillerde algılansa da, bir yandan bireyin dijital ortamda mahremiyetinin korunmasını sağlayan ve bireysel mağduriyetin yaşanmasına engel olan, diğer taraftan dijital arşivlerde bilgi paylaşımı ve bilgiye erişim özgürlüğü ile çatışabilen bir hak olarak da algılanmaktadır. Bireyin gizlilik hakkı ile bireyin ve kamunun bilgiye erişim hakkı arasındaki ince bir çizgi üzerinde yer alan unutulma hakkı, dijitalleşme sürecinde farklı hak ve menfaatler arasındaki dengenin kurulmasını gerektirmektedir. Ancak, farklı tartışmaların odak noktası olan bu hakkın, günümüzde henüz yeterli netlikte anlaşılmadığı ve dijital ortamda ve arşivlerde ne tür içeriklerin hangi şartlarda kaldırılabileceğinin netleşmediği de unutulmamalıdır. Bu çalışmada; dijital ortamda kişisel verilerin korunması ve veri koruma kuralları çerçevesinde günümüzde birçok eleştirinin odak noktası haline gelen unutulma hakkı incelenmiştir. Çalışma kapsamında;

unutulma hakkı kavramını ortaya çıkışından bugüne farklı bakış açıları ile irdeleyen ulusal ve uluslararası hukuksal düzenlemeler ve bilimsel çalışmalar, içerik analizi yöntemiyle incelenerek değerlendirilmiştir. Bu kapsamda; unutulma hakkının bireyin temel bir hakkı olarak değerlendirilmesinin yanı sıra, bilgiye erişim hakkı ve ifade özgürlüğü ile çelişen özelliklerine dikkat çekilmiştir. Unutulma hakkı ve bilgiye erişim özgürlüğü arasındaki çelişkinin ve denge unsurlarının açıklanmasında ise gerçek hayattan yaşanmış hikâyelere ve örnek olaylara yer verilmiştir.

Anahtar Sözcükler: *Unutulma Hakkı, Bilgiye Erişim, Dijitalleşme, Dijital Arşiv, Elektronik Arşiv*

Giriş

Günümüzde, teknolojik gelişmeler bilginin üretilmesi, saklanması, iletilmesi ve paylaşılmasında büyük avantajlar sağlarken, kişisel verilerin korunmasına yönelik endişeleri ve sorunları da beraberinde getirmektedir. Özellikle dünya çapında milyonlarca kullanıcıya hizmet veren internet, bir yandan küresel çapta bilgiye erişim ve iletişim aracı olarak kullanılırken, diğer yandan kişisel verilerin ve dijital mahremiyetin korunması, ifade ve bilgiye erişim özgürlüğü olguları üzerinde şekillenen yeni bir kavramın da "unutulma hakkı" adı altında doğmasına neden olmuştur. Dijital ortamlarda genel itibariyle kişisel verilerin korunmasına ilişkin başlıklar ile gündeme gelen unutulma hakkı (right to be forgotten/oblivion), uluslararası hukukta oldukça tartışmalı ve eleştiriye açık bir konu olarak dikkat çekmektedir. Kişilerin kendileriyle ilgili veriler üzerinde tasarruf edebilmeleri açısından büyük bir önem taşıyan bu hakkın uygulanması ile birlikte yaşanabilecek olumsuzluklara ilişkin en büyük endişe ise, bu hakkın bilgiye erişim özgürlüğünü ihlâl edici bir nitelik taşımasıdır. Bununla birlikte; bir bireyin bilgiye erişim hakkını ihlâl etmeden başka bir bireyin özel hayatın gizliliği hakkını korumanın da oldukça güç olması unutulma hakkına yönelik uygulamaların nasıl benimseneceği konusunda soru işaretlerini de beraberinde getirmektedir.

Bu çalışmada; dijital ortamda kişisel verilerin korunması ve veri koruma kuralları çerçevesinde günümüzde birçok eleştirinin odak noktası haline gelen unutulma hakkı incelenmiştir. Çalışma kapsamında; unutulma hakkı kavramını ortaya çıkışından bugüne farklı bakış açıları ile irdeleyen ulusal ve uluslararası hukuksal düzenlemeler ve bilimsel çalışmalar, içerik analizi yöntemiyle incelenerek değerlendirilmiştir. Bu kapsamda; unutulma hakkının bireyin temel bir hakkı olarak değerlendirilmesinin yanı sıra, bilgiye erişim hakkı ve ifade özgürlüğü ile çelişen özelliklerine dikkat çekilmiştir.

Dijital Mahremiyet ve Unutulma Hakkı

Felsefi, siyasi ve hukuki tartışmalarda sıkça kullanılmasına ve günlük yaşamda çok kullanılan bir terim olmasına rağmen, "mahremiyet"in tek ve basit bir

tanımını yapmak oldukça güç görünmektedir. Bireyin sahip olması gereken en önemli ve değerli hak olarak nitelendirilen mahremiyet, genel olarak bireyin yalnız kalma ve özerkliğini koruma hakkı olarak tanımlanmaktadır (Diffie ve Landau, 2007; Flaherty, 1989; Warren ve Brandeis, 1890). Kökeni ve tarihsel gelişim süreci incelediğinde; sınırları ve taşıdığı anlam, bireyler, toplumlar ve kültürler arasında farklılık gösterse de, temel bir hak olarak kabul edilen mahremiyet kavramının odaklandığı temel olgunun, "gizlilik" olduğunu söylemek mümkündür (DeCew, 2015). Mahremiyeti tek bir boyut altında incelemenin ve sınırlarını kesin olarak tanımlamanın zorluğuna vurgu yapan Belsey (2015), mahremiyeti; bedensel/fiziksel mahremiyet, zihinsel/iletişimsel mahremiyet ve bilgi mahremiyeti olarak sınıflandırmaktadır. Bununla birlikte; kavramın mihenk taşı olan gizliliğin, kişisel özerkliği ifade etmede ve bilgi mahremiyetini ön plana çıkaracak şekilde bireyin kendisi ile bilgileri saklı tutma ve bu bilgilerin kullanımı ve paylaşımı ile ilgili denetim hakkını tanımlamada kullanıldığı görülmektedir (Berman ve Bruening, 2007; Timm ve Duven, 2008).

Mahremiyet, ilk olarak 1890 yılında Amerika Birleşik Devletleri'nde yargıç Louis Brandeis ve avukat Samuel Warren tarafından bireyin yalnız kalma hakkı olarak tanımlanmış (Warren ve Brandeis, 1890); ancak, kavramın kapsamı ve içeriği zaman içerisinde evrilerek, içinde bulunulan çağın özelliklerini yansıtacak bir şekilde genişletilmiştir. Bireylerin kişisel yaşam alanlarını ve gizliliklerini koruma isteği, her zaman önem taşımış ve bireyler kişisel bilgilerinin her an herkese açık olmasından rahatsız olmuşlardır. Diğer yandan, bilgi ve iletişim teknolojilerinde yaşanılan değişim ve gelişmelere bağlı olarak yirmi birinci yüzyıl bilgi çağı olmuş ve bilginin işlenmesinde, depolanmasında ve iletiminde bireylere yeni ve neredeyse sınırsız olanaklar sunmuştur. Ancak, gelişen bilgi teknolojilerinin bilginin işlenmesinde ve iletiminde sağladığı avantajların yanı sıra, mahremiyeti tehdit eden yeni unsurların doğmasına ve bireyin kişisel bilgilerini dijital ortamda daha kolay erişilebilir hale getirerek, bireyin bu alandaki denetim mekanizmasının zayıflamasına da neden olduğunu söylemek mümkündür (Hoven, Blaauw, Pieters ve Warnier, 2016). Günümüzde bilgi ve iletişim teknolojilerinin hayatın her alanındaki yaygın kullanımı ile birlikte, mahremiyet kavramının yeni bir boyut kazandığı ve bireylerin kişisel bilgilerinin dijital ortamda kullanımı ve paylaşımı üzerindeki denetim haklarını vurgulayacak şekilde yerini dijital mahremiyet kavramına bıraktığı görülmektedir (Berman ve Bruening, 2007; Henn, 2014; Houle, 2013; Newman ve Bach, 2004; Terwangne, 2012). Özellikle dünya çapında milyonlarca kullanıcıya hizmet veren ve küresel olarak bilgiye erişim ve iletişim aracı olarak kullanılan internet, bir yandan bilgiye erişimde sunduğu sınırsız imkânlar ile birincil bilgi kaynakları arasında yer alırken, öte yandan kişisel bilgilerin ve dijital mahremiyetin korunması üzerine yeni bir tartışmanın da fitilini ateşlemektedir. Bugün bireyler, dijital ortamda kişisel özerkliklerinin korunarak kişisel bilgilerinin paylaşımını kontrol etme ve üçüncü kişiler tarafından kullanımını denetleme hakkına sahip olmayı talep

etmektedirler. Bu noktada, görece yeni, oldukça tartışmalı ve eleştiriye açık bir kavram olarak unutulma hakkı kavramı karşımıza çıkmaktadır.

Genel bir bakış açısıyla ele alındığında, unutulma hakkını; "bireyin dijital ortamda yer alan kişisel verilerinin çeşitli sebeplere bağlı olarak silinmesini ve daha fazla yayılmasının önlenmesini talep etme hakkı" olarak tanımlamak mümkündür (European Commission, 2014). Avrupa'da filizlenmeye başlayan ve daha sonra diğer dünya ülkelerinde de birçok tartışmanın odak noktası haline gelen unutulma hakkının ilk olarak telaffuz edilmesi, her ne kadar hükümlü bireylerin tahliyelerinin ardından cezai geçmişlerinin silinmesini talep etmeleri ile ilgili hukuki süreçler ile gündeme gelse de, günümüzde bu kavramın boyutlarının bireyin adli kayıtlarının çok ötesine geçtiği görülmektedir. Günümüzde, unutulma hakkı özel hayatın gizliliği ve kişisel verilerin korunması hakları kapsamında bir bireyin sahip olması gereken temel bir hak olarak değerlendirilmektedir. Bu nedenle, unutulma hakkının tanımının yapılmasında ve sınırlarının belirlenmesinde dikkate alınması gereken en önemli unsur, kişisel veri kavramının ne ifade ettiğinin anlaşılmasıdır. Ayrıca, bu hak ile bireyin dijital ortamdan kaldırılmasını talep ettiği kişisel verilerin ulusal ve uluslararası hukuk mevzuatı kapsamında nasıl ele alındığı ve korunduğu da konunun detaylandırılması açısından önem taşımaktadır.

Kişisel Veri ve Kişisel Verilerin Korunması Hakkı

Kişisel verilerin korunması amacıyla birçok alanda yasal düzenlemeler yapan Avrupa Birliği'nin 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Tanımlar" başlığı altında yer alan 4/1 maddesinde kişisel veri; "kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri" olarak tanımlamaktadır (European Union, 2016, s. 33). Bu tanım doğrultusunda kişisel veri; bireyin fiziksel, psikolojik, ekonomik, kültürel veya sosyal kimliğine özgü somut bir ya da daha fazla faktöre gönderme yaparak, doğrudan veya dolaylı olarak bireyi tanımlayan veri olarak kabul edilmektedir. Türk hukuk mevzuatında ise 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel veri, söz konusu veri koruma tüzüğü ile benzer bir şekilde; "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmaktadır (T.C. Başbakanlık, 2016, s. 12301). Bu kapsamda kişisel veri kavramı, bireyi doğrudan ve kesin olarak tanımlamayı sağlayan adı, soyadı, doğum tarihi, doğum yeri vb. bilgilerin yanı sıra, fotoğraf, görüntü ve ses kaydı, parmak izi, motorlu taşıt plakası, pasaport numarası, telefon numarası, dini inancı, siyasi görüşü vb. bireyin fiziki, ailevi, ekonomik ve sosyal kimliğini ifade eden somut içerikleri veya bu

tür bir içerik ile ilişkilendirilerek bireyin tanımlanmasını sağlayan tüm durumları ifade etmek için de kullanılmaktadır (Türkiye Büyük Millet Meclisi, 2016).

Kişisel verilerin korunması hakkı, bireyin temel hak ve özgürlükleri kapsamında değerlendirilen ve bireyin özel hayatının gizliliğine ilişkin anayasal bir haktır (T.C. Başbakanlık, 2016). Ancak, bu noktada kişisel verilerin korunmasına ilişkin küresel çapta herhangi yasal bağlayıcı bir unsurun ve denetim mekanizmasının bulunmadığını ve konunun genel olarak bölgesel veya yerel/ulusal nitelikte hukuki düzenlemeler yoluyla, farklı bakış açıları ile ele alındığını belirtmekte fayda vardır.

Ulusal ve uluslararası düzenlemeler yoluyla kişisel verilerin korunmasına yönelik 1970'li yıllardan bu yana süren çalışmaların öncüleri; sırasıyla 1970, 1973 ve 1978 yıllarında ulusal anlamda ilk veri koruma kanunları ile Almanya, İsveç ve Fransa kabul edilmektedir (Kişisel Verileri Koruma Kurumu, 2017b). Kişisel verilerin korunmasına ilişkin uluslararası düzeyde ise; Avrupa Birliği ve Avrupa Konseyi'nin yürüttüğü farklı çalışmalar olmasına rağmen, Avrupa Parlamentosu ve Avrupa Konseyi tarafından 24 Ekim 1995 tarihinde kabul edilen "95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif" ön plana çıkmaktadır. Bu direktif ile Avrupa Birliği'ne üye ülkelerdeki bireylerin kişisel verilerinin korunmasının yanı sıra, üye ülkelerin bu direktifi esas alarak hazırlayacakları veri koruma kanunlarının uyumlaştırılması da amaçlanmıştır (European Commission, 1995). Söz konusu direktif, kişisel verilerin korunması alanında Avrupa Birliği üye ülkelerinin yanı sıra, tüm dünyada kabul gören bir çerçeve plan sunmaktadır. Ancak, modern çağın teknoloji alanında getirdiği yenilikler ile birlikte, direktifte yer alan ilkelerin yeniden düzenlemesi ve güncel teknolojik gelişmelere uyumlaştırılması zorunlu hale gelmiştir. Özellikle gelişen bilişim teknolojileri ile birlikte kişisel verilerin toplanmasının, işlenmesinin ve paylaşımının kolaylaşması ve dijital mahremiyet/güvenlik konularında duyulan endişeler, direktife ilişkin reform çalışmalarına ivme kazandırmıştır (European Commission, 2016). Bu kapsamda Avrupa Birliği'nin 2012 yılında başlattığı tüzük çalışmaları neticesinde; 95/46/EC sayılı direktifin ilga edilmesiyle birlikte 25 Mayıs 2018 tarihinden itibaren geçerli olacak "2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü", 24 Mayıs 2016 tarihinde yürürlüğe girmiştir (European Union, 2016). Tüm bu açıklamalar doğrultusunda Avrupa Birliği'nin kişisel verilerin korunması ve paylaşılmasına ilişkin birtakım düzenlemeler gerçekleştirdiği ve belirlediği ilkeler ile tüm üye ülkelerde kişisel verilerin aynı standartta korunmasını amaçladığı söylenebilir.

Diğer yandan; Amerika Birleşik Devletleri'nde, bireyin ifade ve basın özgürlüğünün çoğu durumda kişisel verilerin korunması hakkının önüne geçtiği görülmektedir. Kişisel verilerin kullanımı ve korunmasına ilişkin ülke genelinde uygulanan tek ve bütüncül bir kanun bulunmamakla birlikte, ülkedeki her eyaletin çoğu zaman birbiri ile çelişen kanun ve yönetmeliklerinin bulunduğu söylenebilir.

Buna ek olarak; birçok devlet kurumu, konuya ilişkin olarak örnek/iyi uygulamalar şeklinde tavsiye kararları düzenlenmekte, ancak bu kararların herhangi bir yasal yaptırım gücü bulunmamaktadır (Jolly, 2017). Avrupa Birliği'nde bireyin kişisel verilerinin korunmasını talep etmesi, anayasal ve temel bir hak olarak kabul edilirken, Amerika Birleşik Devletleri'nde daha farklı bir anlayış benimsenmiştir. Kişisel verilerin korunması konusunda kısıtlayıcı hukuki unsurların oldukça az olduğu ülkede; özellikle kişisel bilgilerin paylaşılması hususunda kamusal yarar, bireysel/özel yarardan üstün görülerek, bilginin kamuoyu ile paylaşımında kamusal yararın olması, yeterli bir ölçüt olarak değerlendirilmektedir (European Parliament, 2015).

Türkiye'de ise; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 2016 yılında yürürlüğe girmesine kadar, kişisel verilerin korunmasına ilişkin bu alanı bütüncül bir şekilde düzenleyen özel bir kanun bulunmamaktaydı. Söz konusu kanunun yürürlüğe girmesinden önce kişisel verilerin korunmasına ilişkin hükümler, farklı mevzuatlar ile düzenlenmekteydi. Günümüzde anayasal bir hak olarak tanımlanan ve özel hayatın gizliliği ile ilişkili olarak değerlendirilen kişisel verilerin korunması hakkının, ülkemizdeki ilk yasal dayanağının Türkiye Cumhuriyeti Anayasası olduğunu söylemek mümkündür. Anayasanın 20. maddesi ile güvence altına alınan özel hayatın gizliliği, teknolojik gelişmelerin bireyin temel hak ve hürriyetlerine yönelik birtakım tehdit unsurlarını da beraberinde getirdiği gerçeği dikkate alınarak yeniden düzenlenmiştir (Kişisel Verileri Koruma Kurumu, 2017a). 12 Eylül 2010 tarihinde gerçekleştirilen halk oylamasının ardından yürürlüğe giren 5982 sayılı Kanun ile anayasada birtakım düzenlemeler yapılmıştır. Yapılan anayasa değişikliği kapsamında; "özel hayatın gizliliği ve korunması" maddesi yeniden düzenlenmiş ve kişisel verilerin korunması temel bir insan hakkı olarak anayasada yer almıştır. Söz konusu düzenleme ile "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar." ifadesi anayasaya dâhil edilmiştir (T.C. Anayasası, 1982, s. 133). Bununla birlikte; 5237 sayılı Türk Ceza Kanunu'nun 135. ve 140 da dâhil olmak üzere devamı maddelerinde, kişisel verilerin hukuka aykırı bir şekilde elde edilmesi, kaydedilmesi, açığa çıkarılması ve yayılması, "suç" olarak tanımlanmış ve bu fiiller yaptırıma bağlanmıştır (Türk Ceza Kanunu, 2004). Buna karşın ülkemizde; Türk Ceza Kanunu ile suç olarak tanımlanmış bu fiillerin, hangi durumlarda hukuka aykırı olarak gerçekleştirilmiş sayılacağı konusunda uzun yıllar boyunca tereddütler yaşanmış ve bu duruma bağlı olarak uygulamada bazı hak ihlallerinin yaşanmasına mahal verilmiştir (Türkiye Büyük Millet Meclisi, 2016). Benzer şekilde; ülkemizde farklı alanlarda birçok hukuksal düzenlemede (Medeni Kanun, Borçlar Kanunu, Bilgi Edinme Kanunu, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik vb.) kişisel verilerin

korunması konusuna değinilmiştir. Ancak, yapılan bu düzenlemeler sadece kendi sınırları içerisindeki problemlere çözüm getirebilmiştir. Bu durum ülkemizde kişisel verilerin korunması alanına bütüncül bir yaklaşım getirecek özel bir kanunun yürürlüğe girmesini zorunlu hale getirmiştir. Bu noktada; Türkiye'de 1980'li yılardan bu yana ulusal ve uluslararası düzeyde yürütülen çalışmalar sonucunda hazırlanan "Kişisel Verilerin Korunması Kanunu Tasarısı" (T.C. Başbakanlık, 2014), 26 Aralık 2014 tarihinde Türkiye Büyük Millet Meclisi Başkanlığı'na sunulmuştur. Kanun tasarısı 24 Mart 2016 tarihinde kabul edilmiş, 7 Nisan 2016 tarih ve 29677 sayılı resmi gazetede yayımlanarak "6698 Sayılı Kişisel Verilerin Korunması Kanunu" (T.C. Başbakanlık, 2016) adı altında yürürlüğe girmiştir.

Unutulma Hakkı Kavramının Ortaya Çıkışı

1972 yılında Carlos Castaneda, doğadışı güçlerinden ötürü Güneybatı Amerika halkının korkup çekindiği bir Yaqui Kızılderilisi olan Don Juan'ın öğretilerini anlattığı kitabında; "En iyisi tüm kişisel tarihimizi silmek çünkü bu bizi diğer insanların düşüncelerinden özgür kılar." (1991, s. 17) ifadesini her ne kadar günümüzün teknoloji ile donatılmış yaşam biçimlerini öngörerek söylemese de bugün bireyler dijital ortamdaki kişisel verilerinin silinmesini ve diğer insanlar tarafından unutulmayı talep etmektedirler. İnsan hafızası ile kıyaslandığında dijital arşivlerin, özellikle de internetin, sonsuz bir saklama kapasitesinin olduğunu ve bu arşivlerde depolanan veya internet ortamında paylaşılan bilgilerin zamanla yok olmayacağını söylemek mümkündür. Bununla birlikte; gelişen bilgi ve iletişim teknolojileri bilginin saklanması ve iletiminde sunduğu avantajların yanı sıra, hem bireysel hem de toplumsal anlamda mahremiyete olan bakış açısını ve normları da değiştirmiştir. Günümüzde bireyler normalde yüz yüze iletişimde paylaşmayacakları kişisel verilerini sosyal medya vb. dijital ortamlarda paylaşmakta herhangi bir sakınca görmemektedirler (Hoven ve diğerleri., 2016). Bu durumda; dijital arşivlerin yanı sıra her bilginin sonsuza dek hatırlanabileceği bir ortam olan internette, bilgi mahremiyeti kapsamında bireyin kişisel verileri üzerinde kontrol hakkının olması büyük önem taşımaktadır. Tam bu noktada ise birçok birey için kurtarıcı bir can simidi görevini üstlenen unutulma hakkının ön plana çıktığı görülmektedir. Özünde bireyin onurlu bir yaşam sürdürme ve kişisel verilerine ilişkin tasarruf etme hakları ile özel hayatın gizliliği yer almasına bağlı olarak; unutulma hakkı günümüzde genellikle kişisel verilerin ve dijital mahremiyetin korunması olguları ile birlikte anılmaktadır. Bu nedenle unutulma hakkı kavramının doğmasında etkili olan olayların genel itibariyle bu iki olgu üzerinde şekillendiği söylenebilir.

Unutulma hakkına ilişkin ilk girişimin Mario Costeja González isimli İspanyol bir avukat tarafından bulunulduğu bilinmektedir. İspanya'da ikamet eden Costeja González, Google arama motorunda kendi ismi ile arama yapılması durumunda;

İspanyol "La Vanguardia" gazetesinin 19 Ocak ve 9 Mart 1998 tarihli ve "Mario Costeja González" ifadesinin yer aldığı iki sayfasına ait bağlantıların çıktığını fark etmiştir. Söz konusu haber sayfalarında Costeja González'in sosyal güvenlik borçları için başlatılan haciz işlemleri nedeniyle bir gayrimenkulünün satışa çıkarıldığına dair ifadeler yer almaktaydı. Costeja González, kendisiyle ilgili haciz işlemlerinin yıllar önce tamamen çözülmüş olduğunu ve bu işlemlere yapılan atıfların artık tamamen ilgisiz olduğunu belirterek, 5 Mart 2010 tarihinde İspanyol Veri Koruma Kurumu (İVKK)'na başvuruda bulunmuştur. Costeja González başvurusunda kişisel verilerinin korunması hakkını gerekçe göstererek; La Vanguardia gazetesinin söz konusu haber sayfalarını kaldırmasını veya haber sayfalarında kişisel verilerinin artık görünmeyeceği bir şekilde değişiklik yapılmasını talep etmiştir. Costeja González başvurusunda ayrıca kendisiyle ilgili kişisel verilerin Google İspanya ve Google Inc. şirketlerinin arama indekslerinden çıkarılmasını talep etmiştir. İVKK, başvurudaki La Vanguardia gazetesiyle ilgili talebi haberin doğru ve yasal olduğu gerekçesiyle reddederken Google İspanya ve Google Inc. şirketlerinin aleyhine yönelik talebi ise kabul etmiştir. İVKK; söz konusu şirketlerin veri işleme faaliyeti yapmalarını bağlı olarak veri koruma mevzuatına tabi olduklarını ve kişisel verilerin korunması hakkı kapsamında ilgili kişinin kişisel verilerinin üçüncü şahıslar tarafından bilinmemesi yönündeki talebinin yerinde olduğunu beyan etmiş ve Google İspanya ve Google Inc. şirketlerinin ilgili bağlantılara erişimin yasaklanması hususunda yükümlü olduklarını hükmetmiştir. Google İspanya ve Google Inc. ise; kararın kamunun bilgi edinme hakkını ihlâl ettiği gerekçesiyle alınan bu karara karşı İspanya Ulusal Yüksek Mahkemesi'ne başvurarak temyiz davaları açmışlardır. Mahkeme, arama motorlarının kişisel verilerin korunmasına ilişkin ne tür sorumluluklarının olduğunun tespit edilmesi amacıyla 95/46/EC sayılı direktife başvurulması gerektiğini belirtmiş ve konu hakkında görüş bildirmesi için Avrupa Birliği Adalet Divanı'na başvurmaya karar vermiştir (European Court of Justice, 2014b).

Divan, konuya ilişkin olarak 13 Mayıs 2014 tarihli kararında 95/46/EC sayılı direktifin ilgili hükümlerine dayanarak; kamunun bilgiye erişiminde üstün bir menfaatin olduğunu kanıtlayan özel nedenlerin bulunmaması halinde bireyin özel hayatın gizliliği hakkının, kamunun bilgi edinme hakkının üzerinde olduğunu belirtmiş ve bireyin kişisel verilerini içeren bağlantıların arama motorunun sonuç listesinden kaldırılmasını talep edebileceğini değerlendirmiştir. Divan, bu gerekçe doğrultusunda Google İspanya ve Google Inc. şirketlerinin kamunun bilgi edinme hakkı üzerinde yaptığı savunmayı reddederken; başvuruya esas olan haberlerin güncelliğini yitirdiğini ve artık eksik, ilgisiz ve hatalı olarak değerlendirilmeleri gerektiğine değinerek, bu durumda; kamunun bilgi edinme hakkının ortadan kalkacağını belirtmiştir. Tüm bu değerlendirmeler neticesinde; Avrupa Birliği Adalet Divanı, Costeja González'in talebinin yerinde ve haklı olduğu sonucuna ulaşmış ve unutulma hakkı kapsamında ilgili bağlantıların arama motorlarının

sonuç listesinden kaldırılmasına hükmetmiştir (European Court of Justice, 2014a).

Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 tarihli kararı (European Court of Justice, 2014a), unutulma hakkının ilk kez hukuksal bir tabana oturtulmasını sağlamakta ve konuya ilişkin ilk içtihadı oluşturarak benzer kararlar için emsal nitelik taşımaktadır. Ancak, unutulma hakkına ilişkin düzenlemelerin Avrupa Birliği kapsamında yapılan daha eski çalışmalara dayandığını söylemek mümkündür. 1995 yılında yürürlüğe giren 95/46/EC sayılı direktifin "Erişim Hakkı" başlıklı 12. Maddesi incelendiğinde; bu maddenin unutulma hakkını destekleyen temel ilkeyi içerdiği görülmektedir. Söz konusu maddede; verinin eksik ya da yanlış olması durumunda bireyin kişisel verilerinin silinmesini talep etme hakkına sahip olduğu belirtilmektedir (European Commission, 1995). Bununla birlikte; unutulma hakkına ilişkin bir diğer önemli düzenlemenin ise Avrupa Komisyonu'nun söz konusu direktife yönelik 2012 yılında başlattığı reform çalışması olduğu görülmektedir. 95/46/EC sayılı direktif, Avrupa Birliği üye ülkelerinin yanı sıra, tüm dünya için kişisel verilerin korunmasına ilişkin çerçeve bir plan sunmasına karşın; üye ülkeler aynı direktifi farklı şekillerde yorumlayarak veri korumaya ilişkin farklı uygulamaları hayata geçirmişlerdir. Ayrıca; gelişen teknolojiler ve küreselleşmenin de etkisi ile verinin saklanması, kullanımı ve veriye erişim yöntemlerinde yaşanan değişimler neticesinde Avrupa Komisyonu, veri koruma kurallarında kapsamlı bir reform hareketine ihtiyaç duymuştur. Bireyin temel hakları kapsamında dijital ortamda da mahremiyetin korunmasını amaçlayan bu reform hareketine yönelik olarak 25 Ocak 2012 tarihinde yayımlanan taslak metinde unutulma hakkı kavramına yer verildiği görülmektedir. Taslak metinde "Unutulma ve Silinme Hakkı" başlıklı 17. Madde ile verilerin uzun bir süredir toplanma amacı kapsamında kullanılmaması, veri sahibinin verinin kullanılması konusunda rızasını geri çekmesi veya verinin kullanılması için yasal bir dayanağın olmaması durumlarında bireye kişisel verilerinin silinmesini talep etme hakkı tanınmıştır (European Commission, 2012). 25 Ocak 2012 tarihli taslak metin, unutulma hakkı kavramının ilk defa açık ve net bir şekilde ifade edildiği düzenleme olması nedeniyle büyük önem taşımaktadır (European Commission, 2014). Ancak; Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 tarihli kararı, taslak metin hayata geçirilmeden unutulma hakkının yasal olarak ele alındığı ilk girişim ve benzer nitelikteki hukuki olaylar için emsal niteliği taşıyan bir karar olarak kabul görmektedir. Unutulma hakkına ilişkin son düzenlemenin ise "2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü" olduğu söylenebilir. 24 Mayıs 2016 tarihinde hayata geçen tüzüğün "Silinme Hakkı ('Unutulma Hakkı')" başlıklı 17. Maddesi ile 95/46/EC sayılı direktifin 12. Maddesi kapsamında bireye tanınan hakların genişletilerek bireyin kişisel verilerinin işlenmesine rızasının bulunmadığı durumlarda bireye bu verilerinin silinmesini veya bundan sonra da işlenmemesini talep etme hakkı tanınmıştır. Bu kapsamda veri sorumlusu bireyin silinmesini talep ettiği kişisel

verileri gecikmeksizin silmekle yükümlü tutulmuştur. Verinin işlenmesi için bireyin rızasının olmaması, unutulma hakkının talep edilebilmesi için geçerli sayılabilecek gerekçelerden sadece bir tanesi olup bu hakkın kullanılabilmesinde etkili olan diğer faktörler tüzükte ayrıntılı bir şekilde tanımlanmaktadır (European Union, 2016). Bununla birlikte; Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 tarihli kararında ve Avrupa Birliği Genel Veri Koruma Tüzüğü'nde; bireyin unutulma hakkına ilişkin taleplerini öncelikle veri sorumlusuna iletmesi gerektiği ve veri sorumlusunun da kendisine iletilen talebi usulüne uygun bir şekilde inceleyerek değerlendirme sorumluluğu olduğu belirtilmektedir. Veri sorulusunun talebi reddetmesi durumunda ise, bireye kişisel verileri korumaya ilişkin denetim mekanizmalarına/kurullarına ve adli makamlara başvurma hakkı tanınmıştır (European Court of Justice, 2014a; European Union, 2016).

Bilgiye Erişim Özgürlüğü Kapsamında Unutulma Hakkının Değerlendirilmesi

13 Mayıs 2014 tarihinde Google İspanya kararı ile Avrupa Adalet Divanı tarafından ilk olarak hukuki boyutta ele alınan ve 24 Mayıs 2016 tarihinde yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü ile yasal hale getirilen unutulma hakkı, ilk bakışta kişilerin sahip olması gereken temel hak ve özgürlükler kapsamında dijital mahremiyetin korunmasına yönelik olumlu bir adım olarak görülse de; kişilerin/kamunun bilgiye erişim özgürlüğüne zarar vereceği ve dijital ortamda iletişim ve ifade özgürlüğünü engelleyeceği de sıkça dile getirilmektedir. Avrupa Birliği kapsamında yapılan yasal düzenlemeler ile unutulma hakkının kapsamı ve sınırları çizilerek bu hakkın istisnai durumları arasında ifade özgürlüğüne ve bilgiye erişim hakkına yer verilse de; hem unutulma hakkı hem de ifade özgürlüğü ve bilgiye erişim hakkı uygulanma süreci açısından uluslararası boyutta farklı şekillerde algılanabilmekte ve bu hakların dengesi üzerindeki tartışmalar teoriden gerçek hayata geçirildiğinde durum karmaşık bir hal alabilmektedir. Bununla birlikte, Amerika Birleşik Devletleri'nde kişisel verilerin korunması hususuna ilişkin Avrupa Birliği'nden daha farklı bir anlayışın benimsenmesi neticesinde; unutulma hakkı, ifade özgürlüğü ve bilgiye erişim hakkı arasındaki dengenin kurulmasında kıtalar arasında da çelişkilerin yaşanması söz konusu olabilmektedir.

Avrupa Adalet Divanı, Google İspanya kararı kapsamında 95/46/EC sayılı direktifin hükümlerine dayanarak unutulma hakkının çerçevesini tanımlarken; bu hakkın uygulanmasında birtakım istisna durumların olabileceğini ve bu karar ile verilen hükmün benzer durumlar için mutlak olmadığını belirtmiştir. Söz konusu kararda; dava konusu olayda veya benzeri taleplerde değerlendirme yapılırken arama motorlarının ekonomik menfaatlerinin yanı sıra, birey tarafından silinmesi talep edilen bilginin niteliği, bireyin toplum içerisindeki konumu ve kamunun

bilgiye erişim hakkı olgularının da dikkate alınmasının gerekliliğinden bahsedilmektedir. Kararda; bireyin kişisel verilerini içeren bağlantıların arama motorundan kaldırmasını talep etmesi durumunda, söz konusu bu bilgiye erişmek isteyen internet kullanıcılarının meşru menfaatleri ile bireyin kişisel bilgilerinin korunması ve özel hayata saygı hakları arasında adil bir dengenin kurulmasının gerekliliğinden bahsedilmektedir. Bununla birlikte kararda; bireyin temel hakları kapsamında değerlendirilen bu iki hak, genel olarak internet kullanıcılarının bilgiye erişimdeki meşru menfaatlerinden üstün görülürken; adil bir dengenin kurulmasının söz konusu bilginin niteliğine, bireyin özel yaşamında taşıdığı değere / hassasiyet durumuna ve kamunun bu bilgiye erişiminde bireyin toplumda üstlendiği role bağlı olarak değişebilen menfaatlerine bağlı olduğu belirtilmiştir (European Court of Justice, 2014a). Benzer şekilde; 95/46/EC sayılı direktifin reform çalışmaları kapsamında hazırlanan taslak metinde ve bu direktifi ilga ederek yürürlüğe konulan Avrupa Birliği Genel Veri Koruma Tüzüğü'nde unutulma hakkının istisnaları tanımlanmıştır. Avrupa Komisyonu'nun taslak metninde, unutulma hakkının hangi durumlarda uygulanabileceği tanımlanırken, bu hakkın istisnaları olarak ifade özgürlüğüne ve bilgiye erişim hakkına atıfta bulunulduğu görülmektedir. Taslakta bir yandan unutulma ve silinme hakkı kapsamında belirtilen şartların sağlanması durumunda bireyin kişisel verilerin silinmesini talep etme hakkına sahip olduğu belirtilirken, diğer yandan da ifade özgürlüğünün korunabilmesi adına verilerin tarihsel, istatiksel veya bilimsel araştırma amacıyla kullanıldığı durumlarda ya da kamu sağlığını ilgilendiren bir konuda söz konusu verinin silinmesinin kamu yararına engel olacağı öngörülen durumlarda veri sorumlusunun bu veriyi tutma/saklama hakkının olabileceğine değinilmektedir (European Commission, 2012). Avrupa Birliği Genel Veri Koruma Tüzüğü'nde de benzer bir şekilde unutulma hakkının uygulanış biçiminin mutlak olmadığı vurgulanarak, bireyin silinmesini talep ettiği verilerin bazı istisna durumlarda saklanmaya ve işlenmeye devam edebileceği hükmedilmiştir. Bu istisnai durumların arasında ise; ifade ve bilgi özgürlüğünün kullanılmasının yanı sıra kamu yararı doğrultusunda arşivleme çalışmalarının, bilimsel ve tarihsel araştırmalarının ve istatistiksel amaçların yer aldığı görülmektedir (European Union, 2016).

Bilgiye erişim özgürlüğü kapsamında unutulma hakkının değerlendirilmesi amacıyla Amerika Birleşik Devletleri'ndeki (ABD) uygulamalar incelendiğinde ise; bilgiye erişimde kamusal yararın olmasının unutulma hakkına ilişkin taleplerin reddedilmesi için yeterli bir gerekçe olarak kabul edildiği görülmektedir (European Parliament, 2015). Bu kapsamda; kişisel verilerin silinmesinin talep edildiği hukuki olaylar ele alındığında, yargı makamlarının özellikle kamu nezdinde haber değeri taşıyan olaylar söz konusu olduğunda ifade ve basın özgürlüğünü gerekçe göstererek, bireysel/dijital mahremiyet hakkının aleyhinde hükümler verdikleri görülmektedir (Bennett, 2012). İfade ve basın özgürlüğü

çerçevesinde şekillendirilen bu hükümlerin ise genel itibariyle kamunun bilgi edinme hakkı ile ilişkilendirildiği söylenebilir.

Unutulma hakkının bilgiye erişim hakkı/özgürlüğü ile çeliştiği yönünde tartışmaların yaşanmasına neden olan en dikkat çekici ve sembolik olaylardan biri Wikipedia davasıdır. Söz konusu bu dava, kimine göre unutulma hakkı ile ifade özgürlüğü ve bilgiye erişim hakkı arasındaki bir çelişkiyi, kimine göre ise bireysel ve kamusal menfaatlerin çatışmasını simgelemesinin yanı sıra; Avrupa Birliği ve Amerika Birleşik Devletleri arasındaki konuya ilişkin farklı bakış açılarını da ortaya koymaktadır. Wolfgang Werlé ve Manfred Lauber ile Wikipedia arasındaki hukuk savaşı olarak nitelendirilen bu dava; Alman aktör Walter Sedlmayr'i öldürmekten hüküm giymiş iki kardeşin Wikipedia nezdinde unutulma haklarını talep etmeleri üzerinde şekillenmektedir. Walter Sedlmayr cinayetinin sanıkları olarak hapis cezasına çarptırılan Wolfgang Werlé ve Manfred Lauber; tahliyelerinin ardından aralarında Wikipedia sitesinin de bulunduğu bir dizi web sitesinden isimlerinin silinmesi talebiyle dava açmışlardır. Wolfgang Werlé ve Manfred Lauber başlattıkları hukuk mücadelesi kapsamında 27 Ekim 2009 tarihinde Wikipedia sitesinin içerik ve yer sağlayıcısı Wikimedia Foundation Inc.'a da bir ihtarname göndererek isimlerinin Walter Sedlmayr cinayeti ile bir daha anılmamasını talep etmişler ve bu durumun kötü şöhretle tanınmalarına neden olarak tahliyelerinin ardından yeni bir hayata başlamalarında engel teşkil ettiklerini ifade etmişlerdir (Stopp & Stopp Law Firm, 2009). Wikimedia Foundation Inc.'a gönderilen ihtarname ile Wolfgang Werlé ve Manfred Lauber, kişisel mahremiyeti koruyan Alman yasalarına dayanarak ve kişilere cezai sürelerini tamamlamalarının ardından mahkûmiyetleri hakkında haber yapılmamasını talep etme haklarının olduğuna hükmedildiği 1973 tarihli bir davayı emsal göstererek; kendilerini Walter Sedlmayr'in katili olarak tasvir eden Wikipedia makalelerinden isimlerinin kaldırılmasını ve Walter Sedlmayr olayının anonimleştirilerek sunulmasını talep etmişlerdir. Söz konusu davada; Hamburg Mahkemesi'nin Wolfgang Werlé ve Manfred Lauber'in isimlerinin bu şekilde anılmasının özel hayatın gizliliğini ihlâl ettiğine, bu kişilerin cezalarını tamamlayarak topluma karşı borçlarını ödediklerine ve bu nedenle de ilgili makalelerden bu kişilerin isimlerinin kaldırılmasına karar vermesinin ardından Alman Wikipedia sitesi Walter Sedlmayr ile ilgili içerik sayfasından Wolfgang Werlé ve Manfred Lauber isimlerini kaldırmıştır. Ancak, aynı talep merkezi Amerika Birleşik Devletleri'nde olan ve İngilizce yayın yapan Wikipedia sitesine yöneltildiğinde, Wolfgang Werlé ve Manfred Lauber kardeşler istedikleri sonucu alamamışlar ve talepleri reddedilmiştir. Wikimedia Foundation Inc. yetkilileri; Almanca yayın yapan Wikipedia sitesinin editörlerinin özel hayatın gizliliği ve kamunun bilgiye erişim hakkı arasında tercihlerini bireyin mahremiyeti yönünde kullanabileceklerini ve bu karara saygı duyacaklarını; ancak, İngilizce yayın yapan Wikipedia sitesinin editörlerinin de ifade özgürlüğü çerçevesinde bu iki isme ait içeriği yayından kaldırmama kararını vermekte özgür olduklarını ve

böyle bir karar vermeleri durumunda da editörleri destekleyeceklerini açıklamışlardır. İngilizce yayın yapan Wikipedia sitesinin editörleri de, Wolfgang Werlé ve Manfred Lauber isimlerinin içerik sayfasından kaldırılmasının ifade özgürlüğünü ve dolayısıyla da kamunun bilgi edinme ve haber alma hakkını ihlâl ettiğini gerekçe göstererek, söz konusu talebi reddetmişlerdir. Wolfgang Werlé ve Manfred Lauber ile Wikimedia Foundation Inc. arasında bir hukuk savaşına dönüşen bu olayda; Alman Wikipedia sitesi tercihini özel hayatın gizliliği ve mahremiyetin korunması lehinde kullanmış görünse de, 2009 yılında Alman Anayasa Mahkemesi'nin Hamburg Mahkemesi tarafından verilen kararı anayasal bir hak olan ifade özgürlüğünü ihlâl ettiği gerekçesi ile bozmasının ardından, Alman Wikipedia sitesi daha önce kaldırdığı içeriği tekrar erişime açmıştır (Arthur, 2009; Schwartz, 2009).

Unutulma hakkı ilk bakışta bireylere dijital arşivlerde kendilerine ilişkin bilgileri kontrol etme yetkisi tanıyarak bu bilgilerin ne zaman, nasıl ve hangi ölçüde üçüncü kişiler ile paylaşılacağına karar vermeyi sağlayan bir hak olarak algılansa da; Wikipedia davasında da görüldüğü üzere, bu hakkın kullanımı ile kamuya açık olan bilgiye erişimin kısıtlanması söz konusu olduğunda birtakım problemleri de beraberinde getirmektedir. Bireysel bir bakış açısı ile değerlendirildiğinde kişi için utanç verici, onur kırıcı ve haysiyeti zedeleyici nitelikte olan bilgiler, çoğu durumda başta tarih araştırmacıları, arşivciler ve kütüphaneler olmak üzere kamu için önemli olabilmekte ve bu bilgilere erişimin kısıtlanması ulusal ve uluslararası boyutta gerçekleşen olaylara ilişkin kolektif hafızayı eksik bırakabilmektedir.

Yapılan yasal düzenlemeler ile istisnaları düzenlenen unutulma hakkının temelinde yatan ana fikrin, toplanma/oluşturulma amacı kapsamında bilginin zaman içerisinde önemini ve işlevsel yararını yitireceği ve bu nedenle de bilginin silinmesinin veya erişimden kaldırılmasının talep edilebileceği olduğunu söylenebilir. Bu bağlamda; Avrupa'da birçok ülkede yasal düzenlemeler ile özellikle hükümlü bireylerin tahliyelerinin ardından topluma uyumlarını sağlayabilmek ve rehabilitasyonları amacıyla cezai kayıtların silinmesi sağlanmakta ve zaman aşımı nedeniyle bireyin mahremiyetini ihlâl eden ve itibarını zedeleyen bilgiye erişimin talep edilemeyeceği belirtilmektedir. Ancak; bu tür bilgilerde de dâhil olmak üzere bazı bilgilerin toplanarak arşivlenmesinin ve tarihsel bir süreç içerisinde erişilebilir olmasının da kamunun bilgi alma ve bilgiye erişim hakkının korunabilmesi adına önem taşıdığı da göz ardı edilmemelidir (Article 19 Free Word Centre, 2016). Kamunun bilgiye erişiminde önemli bir rol üstlenen kütüphanelerin, ulusal arşivlerin ve gazetelerin, sıradan bireylere ait olan kişisel bilgiler de dâhil olmak üzere her türlü bilginin arşivlendiği birer bilgi deposu oldukları bilinmektedir. Ancak ulusal arşivler, tarihsel bir arşivin oluşturulabilmesi veya araştırma yapılabilmesi amacıyla belirli türde bilgileri kalıcı olarak saklayabilseler de, veri koruma çerçevesinde yasal düzenlemelere tabi olmaları nedeniyle bireyin mahremiyet ve gizlilik hakkının ihlâl edilmesi durumunda bu tür bilgiye erişimi kısıtlayabilmekte veya bilgiyi

kayıtlardan silebilmektedirler. Benzer şekilde, gazeteler de haber arşivleri üzerinde veri koruma prensipleri doğrultusunda belirli kısıtlamalara gidebilmektedirler (The National Archieves of Scotland, 2010). Bu durum, ifade özgürlüğü ve bilgi alma hakkı ile çoğu zaman çelişen bir uygulama olarak algılanmaktadır. Fikir, düşünce ve bilginin serbest dolaşımı üzerinde şekillendirilen ifade ve bilgi alma özgürlüğü; sadece bilginin serbest bir şekilde ifade edilebilmesini değil aynı zamanda bireysel ve toplumsal temelde bilgiye herhangi bir kısıtlama olmaksızın erişebilmeyi de kapsamaktadır (Council of The European Union, 2014). Bu açıdan değerlendirildiğinde; ifade ve bilgi alma özgürlüğü ile mahremiyetin ve gizliliğin korunması üzerinde temellendirilen unutulma hakkı arasında bir dengenin kurulmasının oldukça çetrefilli olduğunu söylemek mümkündür. Uluslararası insan hakları kapsamında hem ifade ve bilgi alma özgürlüğü hem de mahremiyetin ve gizliliğin korunması teminat altına alınmış ve her iki hakkın da ihlâlinde yaşanılacak mağduriyetin telafisi zorunlu kılınmıştır (European Court of Human Rights, 1953; United Nations, 1948). Bu durumda, özellikle erişimine kısıtlama getirilmek istenen veya tamamen silinmesi talep edilen bilginin hem bireysel hem de kamusal açıdan önem taşıdığı hallerde; bir tarafta ifade ve bilgi alma özgürlüğünü korumak diğer tarafta ise bireye tanınan unutulma hakkının icrasını sağlamak oldukça zor görünmektedir. Bununla birlikte; mahremiyetin ve gizliliğin korunması kapsamında bireyin kişisel verilerinin korunmasını talep etmesi bireye yasalar ile tanınan temel bir hak olmasına karşın, bireyin bilgiyi sadece kendisine ilişkin olduğu gerekçesi ile kendi mülkü olarak görüp bu bilginin kontrolünün yalnız kendisinde olmasını talep edemeyeceğine ve kişisel nitelikteki bilginin bireysel açıdan önem taşımasının yanı sıra kamusal açıdan da önem taşıyabileceğine ilişkin savlar da unutulma hakkına yönelik tartışmalarda kabul görmeye başlamıştır. Bu tür tartışmalarda bireyin, üçüncü kişiler tarafından paylaşılan kişisel bilgilerinin bireyin onur ve haysiyetine zarar vermesinin haricinde başka nedenlerle silinmesini veya erişiminin kısıtlanmasını talep etme hakkının olmaması gerektiği ve sadece birey merkezli bir yaklaşım ile bilginin ele alınmasının kamunun bilgiye erişim hakkını göz ardı etmek anlamına geleceği savunulmaktadır. Ayrıca, bireysel anlamda ele alındığında önemsiz veya değersiz olarak nitelendirilebilecek bazı bilgilerin toplumsal ve kültürel açıdan önem taşıyabileceği ve hâlihazırda kamuya açık olan bilgilere unutulma hakkı kapsamında erişimin engellenmesinin araştırma ve arşivleme amacıyla yapılan çalışmaları sekteye uğratacağı da bu tür tartışmalarda öne sürülmektedir. Bununla beraber; veri korumaya ilişkin otoriteler de tarihsel ve kültürel bilgilerin kişisel bilgiler içerseler dahi, unutulma hakkı kapsamı dışında tutulması gerektiğini ve bu tür bilgilerin zaman içerisinde işlevselliklerini yitirseler dahi muhafaza edilmesinin önemini vurgulamaktadırlar (Article 19 Free Word Centre, 2016).

Unutulma hakkı ile bilgiye erişim hakkı/özgürlüğü arasındaki çelişkinin çıkmaza girmesinde Avrupa Adalet Divanı’nın 13 Mayıs 2014 tarihli kararı ile birlikte Google arama motorunun unutulma hakkının hayata geçirilmesine yönelik

başlattığı uygulamaların da etkili olduğunu söylemek yanlış olmayacaktır. Söz konusu karar, bireye arama motorları aracılıyla erişilen kişisel bilgilerinin silinmesini talep etme hakkı tanırken, kararda bu talebin her koşulda mutlak olmadığının ve silinmesi talep edilen bilginin niteliğine göre uygulamanın farklı olabileceğinin belirtilmesi, kararın uygulanmasına ilişkin birtakım belirsizlikleri de beraberinde getirmiştir (Scott, 2014). Bu bağlamda; Avrupa'da en çok kullanılan arama motoru olan Google'ın söz konusu karar doğrultusunda unutulma hakkına ilişkin uygulamaları kamuoyunda eleştirilerin odak noktası haline gelmiştir. Avrupa Adalet Divanı'nın kararının ardından Google, unutulma hakkını kullanmak isteyen bireylerin taleplerini almak üzere çevrimiçi bir sistemi hayata geçirmiş ve bu taleplerin değerlendirilmesinde bireyin gizlilik hakkı ile kamunun bilgi alma hakkı ve bilgiyi dağıtma hakkı arasında dengeyi gözeteceğini belirtmiştir. Google, bu sistem aracılığı ile bireyin kendi adını içeren sorgulara ilişkin belirli sonuçların kaldırılmasını talep etmesi halinde talebin uygun görülebilmesi için bireyin gizlilik haklarının kaldırılması talep edilen arama sonuçlarına ilişkin kamu yararının önüne geçmesinin gerekli olduğunu belirtmiştir (Google Inc., 2014). Bununla birlikte, Google unutulma hakkına ilişkin taleplerin değerlendirilmesinde bireyin unutulma hakkı ile kamunun bilgi edinme hakkı arasında dengenin nasıl sağlanacağına yönelik tavsiye kararları alabilmek amacıyla bir danışma kurulu oluşturmuştur (The Advisory Council to Google on the Right to be Forgotten, 2015). Unutulma hakkının kullanımına yönelik başlattığı bu uygulama ile Google, bir taraftan Avrupa Adalet Divanı'nın kararını hayata geçirirken, diğer taraftan da taleplerin değerlendirilmesinde uyguladığı ölçütlerde şeffaf davranmadığına yönelik eleştiriler çerçevesinde bir bireyin mahremiyetini ve gizliliğini korunurken, diğer bir bireyin bilgi alma hakkının ve bilgiye erişim özgürlüğünün nasıl korunabileceğine ilişkin tartışmaların da fitilini ateşlemiştir (Drummond, 2014). Bu tartışmalar kapsamında kamuoyunda oldukça ilgi gören olaylardan birinin de dünyanın çeşitli bölgelerindeki akademisyenler tarafından Google'a hitaben bir mektubun yazılarak, unutulma hakkına ilişkin taleplerin değerlendirilmesinde şeffaflık çağrısında bulunulmasının olduğu söylenebilir. Bilişim hukuku, teknoloji, veri koruma ve felsefe alanlarında uzman toplam 80 akademisyen tarafından imzalanan açık mektupta; kişisel gizlilik ve bilgiye erişim hakları arasındaki dengeye ilişkin karmaşık kararların verilmesinin, arama motorlarının inisiyatifine bırakıldığı ve bu tür dijital platformların muazzam güçlerini kolaylıkla erişilebilen bilgiler üzerinde nasıl kullandıklarının kamuoyu tarafından da bilinmesinin gerekli olduğu ifade edilmektedir (Goodman, 2015). Bu noktada; Avrupa Adalet Divanı'nın unutulma hakkına yönelik kararının Google ve benzeri diğer arama motorları tarafından uygulamaya geçirilmesi ile birlikte yaşanan belirsizlikler ve uygulamada görülen farklılıklara bağlı olarak, unutulma hakkının bireyin gizlilik hakkı ile bireyin veya kamunun bilgiye erişim özgürlüğü arasındaki ince bir çizgi üzerinde yer aldığını ve bu kapsamda birbiri ile çatışan farklı hak ve menfaatler arasındaki dengenin kurulmasının oldukça güç olduğunu söylemek mümkündür.

Unutulma hakkı ve bilgiye erişim özgürlüğü arasındaki çıkmazın değerlendirildiği bir başka platformun da "Uluslararası Kütüphane Dernekleri ve Kurumları Federasyonu (IFLA)" olduğu görülmektedir. IFLA, unutulma hakkı kavramının hayata geçirilmesinin ardından bu hakkın uygulama sürecinde yaşanılabilecek olumsuzlukların ve problemlerin bilgi profesyonellerinin bakış açısı ile değerlendirilmesi amacıyla bir dizi çalışma başlatmış ve bu kapsamda önerilerini kamuoyu ile paylaşmıştır. Bu kapsamda; IFLA, unutulma hakkına ilişkin bir bildiri yayımlayarak veri gizliliği konusunda bilgi merkezlerinin ve bilgi profesyonellerinin göz önünde bulundurması gereken önemli konuları vurgulamış ve unutulma hakkının uzun vadede bilgiye erişim konusunda yaratabileceği olumsuzluklara ilişkin endişelerini dile getirmiştir. Söz konusu bildiride unutulma hakkının; tarihsel kayıtların bütünlüğü ve erişilebilirliği, ifade özgürlüğü ve bilgiye erişim özgürlüğü açısından birtakım problemleri de beraberinde getireceği ifade edilirken kamuya açık bir mecra olan internetteki bilginin kamu veya profesyonel araştırmacılar için önem taşıyabileceği ve bu nedenle de kasıtlı olarak bilginin gizlenmesinin, kaldırılmasının ya da yok edilmesinin doğru olmadığı vurgulanmaktadır. Bununla beraber; bildiride dile getirilen diğer bir husus ise bilginin erişilebilirliğinin yok edildiği bir durumda bilgiye erişim özgürlüğünün onurlandırılamayacağı ve ancak daha üstün bir kamu yararı ile çelişmediği sürece bireyin gizliliğinin korunmasının savunulabileceğidir (IFLA, 2016b). IFLA, bilgiye erişim özgürlüğünü unutulma hakkı karşında savunurken; Avrupa'da unutulma hakkının kapsamının genişletilmesine ilişkin yaşanan bir gelişme de IFLA bildirisinde bilgiye erişim özgürlüğüne ilişkin dile getirilen endişelerin gerçek hayata yansıması olarak değerlendirilmeye başlanmıştır. Avrupa Adalet Divanı'nın 13 Mayıs 2014 tarihli kararı ile bireyin unutulma hakkını talep etmesi durumunda arama motoru silinmesi istenilen içeriğe sadece yerel aramalar için erişimi engellerken (Google Inc., 2016); Fransa'nın veri koruma politikalarını düzenleyen "Commission Nationale de l'Informatique et des Libertés (CNIL)" kurumu, 2015 yılında aldığı bir karar ile unutulma hakkının kapsamının genişletilmesini ve unutulma hakkı dâhilinde alınan kararların küresel çapta uygulanmasını talep etmiştir (CNIL, 2015). Bu gelişmenin ardından, IFLA açık bir mektup yayımlayarak; internet ortamında yayımlanan bilginin günbegün hızla artığı bir çağda bu ortamdaki bilgilerin keşfedilmesinde ve erişilmesinde arama motorlarının hayati bir rol üstlendiklerini ve erişimine kısıtlama getirilmek istenen içeriğin arama motoru sorgularından tamamen kaldırılmasının bilgiye erişimde büyük problemlerin yaşanmasına neden olacağını ifade etmiştir (IFLA, 2016a). Unutulma hakkının mevcut uygulamaları kapsamında; bilgi orijinal kaynağından silinmezken arama motorunda bu hakkı talep eden kişinin ismine ilişkin yapılan sorgudan bu bilgiye erişimi sağlayan bağlantıların kaldırılması söz konusudur (Google Inc., 2016). Bu durumda, bilgi orijinal kaynağında hâlâ ulaşılabilir olduğu için bilgiye farklı bir arama motoru kullanılarak veya talepte bulunan kişinin isminin haricinde anahtar kelimeler kullanılarak erişilmesi mümkündür. IFLA yayımladığı açık mektupta,

CNIL tarafından alınan kararın hayata geçirilmesi durumunda; sadece bir ülkede değil, dünya çapında her yerde ve herkes için bilgiye erişimin sistematik olarak engellenmesinin söz konusu olacağını ve bu durumun da araştırmacılar için büyük bir sorun teşkil edeceğini belirtmektedir. Bununla birlikte; mektupta IFLA bireysel gizliliğin korunmasını desteklediğini ifade ederken, unutulma hakkına ilişkin verilen kararlarda arama motorlarının daha şeffaf bir politika izlemelerinin gerekli olduğunu, gizlilik ile bilgiye erişim özgürlüğü arasında adil bir dengenin kurulmasının önemli olduğunu ve bu süreçte uygulanacak şeffaflığın da unutulma hakkına ilişkin alınan kararların basitleştirilerek uygulanması anlamını taşımayacağını vurgulamaktadır (IFLA, 2016a).

Bu noktada, unutulma hakkına ilişkin gerek Avrupa Birliği gerekse Amerika Birleşik Devletleri kapsamında alınan kararlar ve hayata geçirilen uygulamalar dikkate alındığında; teoride oldukça olumlu bir gelişme olarak ele alınan bu hakkın genel itibariyle bireylerin ifade özgürlüğü ve bilgiye erişim haklarına bir tehdit olarak algılandığını söylemek mümkündür. Unutulma hakkının hayata geçirilme süreci kuramsal boyutta ele alındığında; bilgiye erişimde kamusal bir yararın olmasının bireyin gizlilik hakkından daha üstün olduğu değerlendirilmekte ve bu durumun bilgiye erişim özgürlüğü için bir can simidi olduğu kabul edilmektedir. Ancak, unutulma hakkının gerçek hayatta uygulama boyutu değerlendirildiğinde ise; hangi hakkın daha üstün olduğuna ilişkin kararın verilmesinde kullanılacak ölçütlerin nesnel bir şekilde açık ve net olmadığı görülmektedir. Bu durum ise unutulma hakkının farklı koşullarda farklı şekillerde ele alınmasına ve bilgiye erişim özgürlüğünü koruyarak bu hakkın uygulanması sürecinin oldukça zor ve karmaşık bir hal almasına neden olmaktadır.

Sonuç ve Değerlendirme

13 Mayıs 2014 tarihinde Google İspanya kararı ile Avrupa Adalet Divanı tarafından ilk olarak hukuki boyutta ele alınan ve 24 Mayıs 2016 tarihinde yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü ile yasal hale getirilen unutulma hakkı, dijitalleşme sürecinde farklı hak ve menfaatler arasındaki dengenin nasıl kurulması gerektiğine yönelik birçok soru işaretini de beraberinde getirmiştir. Bireyin gizlilik hakkı ile bireyin ve kamunun bilgiye erişim hakkı arasındaki ince bir çizgi üzerinde yer alan bu hak, kuramsal açıdan bakıldığında kişilerin sahip olması gereken temel hak ve özgürlükler kapsamında dijital mahremiyetin korunmasına yönelik olumlu bir adım olarak görülse de; uygulamaya geçirildiğinde bilgiye erişim özgürlüğüne zarar verdiği ve dijital ortamda iletişim ve ifade özgürlüğünü engellediği gerekçesi ile de oldukça tartışmalı bir hal almıştır. Bununla birlikte; Avrupa Birliği ülkelerinde yasal düzenlemeler ile sınırları kesin bir şekilde çizilen unutulma hakkı, kapsamı ve uygulanma süreci açısından uluslararası boyutta farklı şekillerde algılanmakta, bu

durum da unutulma hakkının uygulanmasına ilişkin süreci daha çetrefilli bir hale getirmektedir.

Avrupa Birliği kapsamında unutulma hakkına ilişkin yapılan yasal düzenlemeler (European Court of Justice, 2014a; European Union, 2016) çerçevesinde; bu hakkın her durum ve koşulda uygulanabilecek mutlak bir hak olmadığı vurgulanırken, istisnai durumlar arasında ifade özgürlüğüne ve bilgiye erişim hakkına yer verilmektedir. Ancak, unutulma hakkının ortaya çıkışında ve zaman içerisinde şekillenmesinde etkili olan hukuksal olaylar (CNIL, 2015; European Court of Justice, 2014a; Stopp & Stopp Law Firm, 2009) incelendiğinde; gizliliğin korunması ve bilgiye erişim özgürlüğü çerçevesinde kişinin yararı ile kamunun yararı arasındaki menfaat dengesinin kurulmasının oldukça zor ve tartışmaya açık bir konu olduğu görülmektedir. Yapılan yasal düzenlemeler ile bu menfaat dengesinin kurulmasında söz konusu bilginin doğasının, bilginin bireyin özel yaşamında taşıdığı değerin, hassasiyet durumunun ve bu bilgiye erişilebiliyor olmadaki kamu yararının dikkate alınması gerektiği tavsiye edilse de; hangi durumlarda ve hangi ölçütler doğrultusunda bilgiye erişimdeki kamu yararının bireyin gizlilik hakkından üstün görüleceği açık ve net değildir. Unutulma hakkına ilişkin taleplerin yöneltildiği otoritelerin başında gelen arama motorlarının talepleri değerlendirirken gözettikleri menfaat ölçütlerinde şeffaf davranmadıkları yönelik eleştiriler (Goodman, 2015; IFLA, 2016b) de unutulma hakkının bir bireyin bilgiye erişim hakkını ihlal etmeden başka bir bireyin özel hayatın gizliliği hakkını koruyarak uygulanabilirliğine de gölge düşürmektedir. Bununla birlikte; 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (European Union, 2016) kapsamında unutulma hakkının sadece Avrupa Birliği ülkelerinde uygulanıyor olması da bu ülkeler dışındaki diğer bölgelerde konuya ilişkin ne tür uygulamaların benimsenerek hayata geçirileceği konusunda soru işaretleri yaratmaktadır. Bu noktada; farklı tartışmaların odak noktası haline gelen unutulma hakkının günümüzde henüz yeterli netlikte anlaşılmadığını ve kuramsal temelde bireyin temel hak ve özgürlükleri kapsamında bireye fayda sağlayacağı öngörülen bu hakkın bilgiye erişim özgürlüğü de dâhil olmak üzere diğer hak ve özgürlüklerle dengelenerek uygulanmasının zaman alacağını söylemek mümkündür.

Kaynaklar

Arthur, C. (2009). *Wikipedia sued by German killers in privacy claim*. 5 Ağustos 2017 tarihinde https://www.theguardian.com/technology/2009/nov/13/wikipedia-sued-privacy-claim adresinden erişildi.

Article 19 Free Word Centre. (2016). The “Right to be forgotten”: Remembering freedom of expression - Policy brief. 6 Mayıs 2017 tarihinde https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf adresinden erişildi.

Belsey, A. (2015). Privacy, publicity and politics. In A. Belsey ve R. Chadwick (Eds.), *Ethical issues in journalism and the media* (pp. 77-92). London: Routledge.

Bennett, S. C. (2012). The "Right to Be Forgotten": Reconciling EU and US perspectives. *Berkeley Journal of International Law, 30*(1), 161 - 195.

Berman, J. ve Bruening, P. (2007). Is privacy still possible in the twenty-first century? *Social Research, 68*(1), 306-318.

Castaneda, C. (1991). *Journey to Ixtlan: The lessons of Don Juan* (1st Washington Square Press trade paperback ed.). New York: Washington Square Press.

CNIL. (2015). *CNIL orders Google to apply delisting on all domain names of the search engine*. 27 Ağustos 2017 tarihinde https://www.cnil.fr/fr/node/15790 adresinden erişildi.

Council of The European Union. (2014). EU Human rights guidelines on freedom of expression online and offline. 6 Nisan 2017 tarihinde https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf adresinden erişildi.

DeCew, J. (2015). Privacy. *The Stanford encyclopedia of philosophy, Spring 2015 Edition*, 28 Ağustos 2017 tarihinde https://plato.stanford.edu/entries/privacy/ adresinden erişildi.

Diffie, W. ve Landau, S. (2007). *Privacy on the line - The politics of wiretapping and encryption*. London: Massachusetts Institute of Technology.

Drummond, D. (2014). *We need to talk about the right to be forgotten*. 18 Haziran 2017 tarihinde https://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate adresinden erişildi.

European Commission. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. 18 Nisan 2017 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF adresinden erişildi.

European Commission. (2012). *Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. 13 Mayıs 2017 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf adresinden erişildi.

European Commission. (2014). *Factsheet on the 'Right to be forgotten ruling' (C-131/12)*. 7 Nisan 2017 tarihinde http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf adresinden erişildi.

European Commission. (2016). *Reform of EU data protection rules*. 25 Haziran 2017erişildi.

European Court of Human Rights. (1953). European convention on human rights. 16 Nisan 2017 tarihinde http://www.echr.coe.int/Documents/Convention_ENG.pdf adresinden erişildi.

European Court of Justice. (2014a). C-131/12: Google Spain v AEPD and Mario Costeja Gonzalez., 12 Nisan 2017 tarihinde

http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 adresinden erişildi.

European Court of Justice. (2014b). Press Release No 70/14: Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. 16 Mayıs 2017 tarihinde https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf adresinden erişildi.

European Parliament. (2015). *A comparison between US and EU data protection legislation for law enforcement purposes*. 25 Mayıs 2017 tarihinde http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf adresinden erişildi.

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the rotection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. 15 Mayıs 2017 tarihinde http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN adresinden erişildi.

Flaherty, D. H. (1989). *Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States*. United States of America: University of North Carolina Press.

Goodman, E. P. (2015). *Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data*. 11 Temmuz 2017 tarihinde https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd adresinden erişildi.

Google Inc. (2014). *Request removal of content indexed on Google Search based on data protection law in Europe*. 19 Nisan 2017 tarihinde https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636435739321993356-2563153326&hl=en&rd=1 adresinden erişildi.

Google Inc. (2016). *Adapting our approach to the European right to be forgotten*. 13 Haziran 2017 tarihinde https://blog.google/topics/google-europe/adapting-our-approach-to-european-rig/ adresinden erişildi.

Henn, S. (2014). *If There's Privacy In The Digital Age, It Has A New Definition*. 7 Haziran 2017 tarihinde http://www.npr.org/sections/alltechconsidered/2014/03/03/285334820/if-theres-privacy-in-the-digital-age-it-has-a-new-definition adresinden erişildi.

Houle, D. (2013). *Is privacy dead? The future of privacy in the digital age*. United States of America: David Houle & Associates.

Hoven, J., Blaauw, M., Pieters, W. ve Warnier, M. (2016). Privacy and information technology. *The Stanford Encyclopedia of Philosophy, Spring 2016 Edition*, 6 Haziran 2017 tarihinde https://plato.stanford.edu/entries/it-privacy/ adresinden erişildi.

IFLA. (2016a). Application of right to be forgotten rulings: The library viewpoint. 5 Temmuz 2017 tarihinde

https://www.ifla.org/files/assets/faife/statements/161024_ifla_on_rtbf_case_in_france.pdf adresinden erişildi.

IFLA. (2016b). IFLA Statement on the right to be forgotten. 12 Mayıs 2017 tarihinde https://www.ifla.org/publications/node/10320 adresinden erişildi.

Jolly, L. (2017). Data protection in the United States: Overview. *Thomson Reuters Practical Law - A Country Q&A Guide to Data Protection in the United States*, 25 Mayıs 2017 tarihinde https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 adresinden erişildi.

Kişisel Verileri Koruma Kurumu. (2017a). *Kişisel Verilerin Korunması Kanunu ve Uygulanması*. 17 Temmuz 2017 tarihinde http://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf adresinden erişildi.

Kişisel Verileri Koruma Kurumu. (2017b). *Ulusal ve Uluslararası Alanda Kişisel Verilerin Korunmasına Duyulan İhtiyaç*. 17 Temmuz 2017 tarihinde http://kvkk.gov.tr/yayinlar/ULUSAL%20VE%20ULUSLARARASI%20ALANDA%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASINA%20DUYULAN%20%C4%B0HT%C4%B0YA%C3%87.pdf adresinden erişildi.

Newman, A. L. ve Bach, D. (2004). Privacy and regulations in a digital age. In B. Preissl, H. Bouwman ve C. Steinfield (Eds.), *E-life after the dot com bust* (pp. 249-269). Heidelberg: Physica.

Schwartz, J. (2009). *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*. 5 Ağustos 2017 tarihinde http://www.nytimes.com/2009/11/13/us/13wiki.html adresinden erişildi.

Scott, M. (2014). *European Companies See Opportunity in the 'Right to Be Forgotten'*. 5 Mayıs 2017 tarihinde https://www.nytimes.com/2014/07/09/technology/european-companies-see-opportunity-in-the-right-to-be-forgotten.html adresinden erişildi.

Stopp & Stopp Law Firm. (2009). W. Werlé ./. Wikimedia Foundation - Article "Walter Sedlmayr" in the English Version Wikipedia. 27 Haziran 2017 tarihinde https://www.wired.com/images_blogs/threatlevel/2009/11/stopp.pdf adresinden erişildi.

T.C. Anayasası. (1982). *Türkiye Cumhuriyeti Anayasası*. 10 Temmuz 2017 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf adresinden erişildi.

T.C. Başbakanlık. (2014). *Kişisel Verilerin Korunması Kanunu Tasarısı*. 16 Nisan 2017 tarihinde http://www2.tbmm.gov.tr/d26/1/1-0541.pdf adresinden erişildi.

T.C. Başbakanlık. (2016). *6698 Sayılı Kişisel Verilerin Korunması Kanunu*. 18 Haziran 2017 tarihinde http://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf adresinden erişildi.

Terwangne, C. d. (2012). Internet privacy and the right to be forgotten/right to oblivion. *Monograph «VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet», 13*, 109-121.

The Advisory Council to Google on the Right to be Forgotten. (2015). How should one person's right to be forgotten be balanced with the public's right to information? , 25 Temmuz 2017 tarihinde https://archive.google.com/advisorycouncil/ adresinden erişildi.

The National Archieves of Scotland. (2010). Data protection code of practice on archival information. 27 Haziran 2017 tarihinde http://webarchive.nrscotland.gov.uk/20170106021747/http://www.nas.gov.uk/documents/dpaCodeOfPracticeOnArchivalInformation%20pdf.pdf adresinden erişildi.

Timm, D. M. ve Duven, C. J. (2008). Privacy and social networking sites. In R. Junco (Ed.), *Using emerging technologies to enhance student engagement: New directions for student services* (pp. 89-102).

Türk Ceza Kanunu. (2004). *5237 Sayılı Türk Ceza Kanunu*. 23 Haziran 2017 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf adresinden erişildi.

Türkiye Büyük Millet Meclisi. (2016). *Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu*. 26 Nisan 2017 tarihinde https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf adresinden erişildi.

United Nations. (1948). The Universal Declaration of Human Rights. 25 Mayıs 2017 tarihinde http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf adresinden erişildi.

Warren, S. D. ve Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 7 Eylül 2017 tarihinde http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm adresinden erişildi.

3. BÖLÜM

EBYS UYGULAMALARININ BOYUTLARI VE STANDARTLAR

Kurumsal Bilgi ve Belge Yönetiminde Uluslararası Standartlaşma Çalışmaları

Prof. Dr. Özgür KÜLCÜ

Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Özet

Belge yönetimi uygulamaları geliştirilirken öncelikle her kurumun özgün yapısı ve işleyişi, tabi olduğu idari ve yasal koşullar göz önüne alınmak durumundadır. Bu çerçevede geliştirilecek sistemler ile kurumsal işeler ve resmi iletişim belgeler üzerinde sorunsuz bir şekilde yürütülebilmekte. Öte yandan belge yönetimi sistemleri geliştirilirken uluslararası koşullar da göz önüne alınmak durumundadır. Konuya ilişkin 90'lı yıllardan itibaren yaygın olarak kullanılmaya başlanan uluslararası standartların bir kısmı ulusal standartlar Türk Standartları Enstitüsü (TSE) tarafından ulusal standartlara da dönüştürülmüştür. Örneğin uluslararası belge yönetimi standardı ISO 15489, TSE ISO 15489 (2007) koduyla yayımlanmıştır. Ulusal bir standart olarak elektronik belge yönetimi yazılımları için referans modeli olarak ortaya çıkan TS 13298 (2015) standardı da, kamuda idari süreçleri ve belge yönetimi uygulamalarına ilişkin temel düzenlemeler dışında kalan konularda AS 4390, Dod 5015.2, MoReq, ISO 27001 gibi uluslararası standartlara atıfta bulunmaktadır. Değişen idari yapılanmalar, gelişen donanım ve yazılım alt yapıları, belgelerin üretildiği, depolandığı, transfer edildiği ve erişildiği platformlardaki farklılaşmalar ve entegrasyon süreçleri, yeni standartların ortaya çıkmasına ya da mevcut düzenlemelerin revizyonuna duyulan gereksinimi artırmaktadır. Çalışma içerisinde değerlendirilen standartların ortalama 2-3 yıl içerisinde revize edilerek yeniden yayımlandığına tanık oluyoruz. Bu çerçevede çalışmada belge yönetimi uygulamalarını etkileyen ya da doğrudan yönlendiren uluslararası düzenlemeler ve standartlar değerlendirilmektedir. Yukarıdaki genel nitelikli standartlar konuya ilişkin çalışmalarda yaygın olarak kullanılmaktadır. Ancak kurumsal bilgi ve belge yönetimi süreçleri birbiriyle ilişkili pek çok konuyu ve alanı kapsayan çalışmaları gerektirmektedir. Betimsel araştırma yönteminin kullanıldığı çalışma geniş bir literatür incelemesi ve ilgili standartların analizi ile gerçekleştirilmiştir. Çalışmada bu çerçevede kurumsal bilgi ve belge yönetimi süreçlerini etkileyen ya da doğrudan bu süreçlerin yürütülmesinde belirleyici olan standartlar kapsam olarak alınmıştır Çalışma kapsamında ağırlıklı olarak kurumsal bilgi ve belge yönetimi sistemlerinin geliştirilmesinde ya da yürütülmesinde belirleyici olan standartlar yer almaktadır. Bununla birlikte çalışmada bilgi ve belge yönetimi uygulamalarının kapsamına giren ve sistem geliştirme çalışmalarında faydalanılabilecek standartlar da yer almaktadır. Bu çerçevede konya ilişkin geniş bir çerçeve çizmeyi amaçlayan bu çalışmanın ilgili araştırmalara destek vermesi umulmaktadır.

Anahtar Kelimeler: *Kurumsal Bilgi Sistemleri, Belge Yönetimi, Standartlaşma, Ulusal Standartlar, Uluslararası Standartlar.*

Belge Yönetimi Uygulamalarının Çerçevesi

Kurumlarda bilgi ve belge kaynakları iş süreç yönetimi, yapılandırılmış iletişim, denetim ve doğrulama ile karar destek aracı olarak yoğunlukla kullanılmaktadır. Bu kaynakların etkili yönetimi, aynı zamanda kurumsal başarının artırılmasında temel rol üstlenmektedir. Bilgi ve belge yönetim sistemleri insan, sermaye, doğal kaynaklar, hizmet ve ürün gerçekleştirmeye yardımcı araç ve yöntemler kadar iş süreçlerinin başarısına etki edebilmektedir. Yapılandırılmış işi tanımlayan ya da bu çerçevede kullanılan bilgi ve belge kaynakları, yeni çalışmalarda girdiye, süreçle tekrar sentezlenerek ileriki çalışmalar için kullanılabilecek çıktıya dönüşmekte, bu süreç yönetim bilimlerinde temel kalite geliştirme döngüsü olarak benimsenmektedir (Bergman, 1994, s.405; TS EN ISO 9001, 200, s.1). Bu çerçevede uluslararası literatürde kurumsal bilgi ve belge kaynaklarının etkili yönetimine dönük sistemleri ve modelleri betimleyen pek çok çalışma yer almaktadır (Information Management Planning, 2005; Pember, 2006; Thurston, 2005). Öte yandan teknoloji kurumlarda, ağırlıklı olarak bilgi sistemlerini etkilemiş, hatta kurumsal teknolojiler ile bilgi sistemleri özdeşleşmiştir. 1980'li yıllarda kelime işlemcilerden 1990'larda otomasyon uygulamalarına, 2000'li yıllarla iş süreç yönetim ve elektronik belge yönetimi uygulamalarından kurumsal içerik yönetimi (enterprise content management) çözümlerine yönetim, teknoloji ve bilgi sistemleri arasındaki ilişkisi giderek güçlenmektedir (Cimtech Ltd, 2009, ss.10-12; Herrera-Viedma ve Peis, 2003, ss.234-238; Kampffmeyer, 2006, s.3, Külcü 2012).

Geleneksel olarak belgeler kurum içi ve kurumun çevresiyle olan iletişimini sağlayan, uygulamalara kanıt niteliği taşıyan dokümanter kaynaklar olarak kullanılmışlardır (Kunis and Schwind, 2007, s.191; Rosenfeld and Morville, 2002, s. 221). Belgeler tanımlanırken üretildiği ortam ya da formatı değil içerdiği bilginin özgünlüğü ve güvenilirliği belirleyici olmuştur (Reed, 2005, s.41). Uluslararası belge yönetimi standardı ISO 15489 içerisinde de belgeler tanımlanırken kanıt (evidence) nitelikleri ve yasal geçerliliği üzerinde durulmaktadır. Belge yönetimi çalışmaları da kurumsal bilgi hizmetlerinin etkin olarak yürütülmesi olarak adlandırılmaktadır (International Organization for Standardization **ISO 15489-1:2001;** Sundberg, 2007, s.32). Kurumlarda belge yönetimi faaliyetleri resmi iletişim ya da doğrulama amacıyla belgelerin üretiminden (creation) ayıklanmasına (disposition) kadar olan süreci kapsamaktadır (Batley, 2007, s.141). Kurumlar etkinliklerini elektronik ortama taşımalarıyla birlikte belge yönetimi uygulamaları da elektronik ortamda tanımlanmaya başlamıştır. Günümüzde elektronik belgelerin kullanımı son derece hızlı biçimde artmaktadır. Uluslararası belge yönetimi derneği ARMA'nın (ARMA International) ABD'de gerçekleştirdiği çalışmaya göre belgelerin %90'ından fazlası artık elektronik ortamda üretilmektedir (ARMA, 2008; Sundberg, 2007, s.31). Oranın bu denli yüksek çıkmasında 70'li yıllarla kullanılmaya başlayan elektronik posta yoluyla iletişimin etkin olarak kullanımının önemli bir rolü olduğu düşünülmektedir (Külcü, 2009).

Elektronik belge yönetimi bilgi teknolojilerine paralel olarak gelişme şansı bulmuştur. Elektronik belgeler genel olarak bir bilgisayar sistemi bünyesinde üretilen, işlenen ve saklanan belgeleri tanımlamaktadır (Kandur, 1999, s. 16). Elektronik ortamda belgeler, basılı belgeler gibi kanıt niteliği taşıyan, sayısal olarak kodlanmış elektronik verilerden oluşmaktadır. Bu anlamda İnternet üzerinden yapılan hukuki işlemler, e-posta yoluyla gönderilen irade beyanları, çeşitli veri taşıyıcılarına kaydedilmiş ve irade açıklaması içeren elektronik veriler ilk akla gelenler arasındadır (Erturgut, 2004, s.66; Wamukoya and Mutula, 2005, s.71). Elektronik ortamda üretilen dokümanlar arasından elektronik belgeleri ayıran özelliklere yönelik Duranti (2001, s.4) altı unsur üzerinde durmaktadır. Bunlar:

- Belgelerin ortamı,
- İçeriği,
- Fiziksel formu ve formu,
- işlevi - fonksiyonu,
- Arşivsel değeri ve
- Yasal ve idari koşulları olarak sıralanmaktadır.

Elektronik ortamda belgelerin yasal süreçte kanıt niteliği olması için nitelikli elektronik sertifikaya sahip olması, ya da daha genel bir ifadeyle sayısal imzayı içermesi önemli görülmektedir. Avustralya Ulusal Arşivi (National Arvhives of Australia) tarafından hazırlanan belge yönetimi sözlüğünde sayısal imza "sayısal objeleri üretenlerin tanımlanması ve sayısal objeler üzerinde gerçekleştirilen değişikliklerin izlenebilmesi için elektronik belgelere eklenmiş güvenlik mekanizması (Glossary of Records Management Terms, 2008,) olarak tanımlanmıştır. Tanımdan da anlaşılacağı üzere basılı belgelerde olduğu gibi elektronik belgelerin de özgünlüğünü tanımlayan imza benzeri güvenlik unsurlarına sahip olmalıdır (Külcü, 2009).

Ülkemizde de özellikle 2000'li yıllarla birlikte gerek kamu gerekse özel sektör yoğun biçimde *elektronik bilgi ve belge yönetim* (EBBY) uygulamalarına geçmeye yönelmişlerdir (Külcü, 2009). EBBY sistemlerin güvenliğine dönük koşulların gelişmesi, ISO 13298 gibi ulusal düzeyde otorite kaynakların varlığı, bu alanda yetkinleşmiş organizasyonların sayısının giderek artması elektronik sistemlere geçişin hızlanmasına katkı sağlamaktadır. Ülkemizde kurumsal bilgi ve belge yönetimi uygulamalarına dönük literatürün zenginleşmesi de (Çiçek, 2011; İçimsoy, 1997; Özdemirci, 2008; Kandur, 2011; Külcü, 2010; Odabaş, 2007) uygulamalara ilgi ve farkındalığın artışında önemli bir etken olarak görülmelidir. Elektronik ortamda bilgi ve belge işlemlerinin geçerliliğine ilişkin yasal çerçeve 2004 yılında kabul edilen 'Elektronik İmza Kanunu' ile oluşturulmuştur. Resmi iş sürecinin elektronik ortama taşınmasına dönük alt yapı koşulları, elektronik uygulamaların geçerliliğini sağlamaya dönük geliştirilen diğer düzenlemeler ve var olan yasal düzenlemelerdeki iyileştirmelerle (Bilgi Edinme Hakkı Kanunu, 2003; Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik, 2001-2005; Elektronik İmza Kanunu, 2004; Resmi Yazışmalarda

Uygulanacak Esas ve Usuller Hakkında Yönetmelik, 2015; Standart Dosya Planı, 2005; TS 13298, 2015; TS ISO 15489-1-2, 2007) belirli bir düzeye ulaştırılmıştır. Yine sistemlerini elektronik ortama taşıyan kurumların elde etikleri verimlilik düzeyleri de diğer kurumları harekete geçiren olumlu bir etkendir. Kurumlar dijitalleştirme çalışmalarıyla kağıt ortamda belgelerin elektronik ortama taşıyarak ve/veya iş süreçlerinin bütünüyle elektronik ortama yürütülmesine dönük projelerle elektronik belge yönetimi uygulamalarına yönelmektedirler. Elektronik belge yönetimi uygulamaları ile zaman ve mekândan bağımsız eşgüdümlü çalışma koşulları yaratılabilmekte, kurumsal iş süreçleri saniyeler içerisinde tamamlanabilmekte, çoklu erişim ve paylaşım olanakları yanında depolama ve yedekleme sorunları kolayca aşılabilmektedir. Elektronik arşivlerin sağladığı web tabanlı bütünleşik içerik oluşturma ve yayımlama özellikleri de eklendiğinde elektronik belge yönetimi uygulamaları kurumların iş yükünün önemli bir bölümünü karşılayabilmektedir (Külcü 2012).

Belge Yönetiminde Uluslararası Standartlaşma Çalışmaları

Aşağıda belge yönetimi alanında standartlaşma çalışmaları ve bu çerçevede geliştirilen standartlar kronolojik düzen içerisinde incelenmektedir.

Avustralya Ulusal Belge Yönetim Standardı (AS 4390)

Belge yönetimi alanında ulusal boyutta kabul edilen ilk standart olan Avustralya Belge Yönetimi Standardı AS 4390, uluslararası standartların geliştirilmesinde de temel alınmıştır. Standart, çoğunluğu kamu kesiminden gelen arşiv ve belge profesyonelleri ile özel sektör danışmanları, kurumları ve Avustralya Kurum Sekreteryaları Enstitüsü (Institutute of Company Secretaries of Australia)'nün girişimleri sonucu ortaya çıkmıştır. AS 4390 Standardının geliştirilmesine yönelik girişimler, geleneksel veya elektronik ortamda üretilen ve kullanılan belgelerin kodlama standartlarının oluşturulması amacıyla başlatılmıştır. Ancak standardın asıl önemi, kurumsal belge yönetimi uygulamalarını bir bütün olarak ele alarak, tasarımdan nihai ayıklamaya kadar ayrıntılarıyla tanımlamaya yönelmesinde yatmaktadır. AS 4390 Avustralya Belge Yönetimi Ulusal Standardı (Australian National Standard for Records Management) olarak 1996 yılında kabul edilmiştir. Belge yönetimi alanında dünyanın ilk genel standardı olarak kabul edilmektedir (Stephens, 2001, s.70; National Archives of Australia, 2006). Standart genel olarak aşağıda belirtilen amaçlara yönelmektedir:

a. Belge hizmetlerinin yürütüldüğü kurumsal çevrenin analizi,

b. Belge işlemlerinin de dâhil dolduğu iş sürecinin analizi,

c. Hangi belgelerin sağlanacağı, ne kadar süre alıkonulacağına karar vermeye yönelik entelektüel çalışmalar (MacKenzie, 1999:26).

ISO'nun 1998 yılında Atina'da gerçekleştirdiği ABD, Almanya, Avustralya, Danimarka, Fransa, İngiltere, İrlanda, İsveç, Kanada'nın da katıldığı, ARMA, ICA ve IRMC'nin temsil edildiği, 46 Nolu Teknik Komite toplantısı çerçevesinde (ISO'nun belge yönetimi alanında oluşturduğu bir komitedir, 2001 yılında yayımlanan ISO 15489 belge yönetimi standardını bu komite tarafından geliştirilmiştir) uluslararası belge yönetimi standartlardı geliştirilirken AS 4390'ın temel alındığı belirtilmektedir (MacKenzie, 1999, s.28).

ISO 15489 Bilgi ve Dokümantasyon - Belge Yönetimi İçin Standart

ISO'nun Bilgi ve Dokümantasyon Teknik Komitesi'ne (Information and Documentation ISO/TC 46) bağlı Arşiv ve Belge Yönetimi Alt Komitesi (Archive and Records Management, SC 11), 2001 yılında ISO 15489-1 kodlu 'Uluslararası Belge Yönetim Standardını' geliştirmiş ve ISO /TR 15489-2 kodlu Teknik Raporu yayımlamıştır.

ISO 15489, ISO ve çeşitli belge yönetimi örgütlerinin ortak çalışmaları sonucu geliştirilen, belge yönetimine dönük küresel ilk standarttır. ISO 15489, ISO'nun belge yönetim standardı olarak tüm kurumlara yönelik genel içerikli tanımlamalara yer vermektedir. Belge yönetimini kurumsal yönetimin vazgeçilmez bir uygulama alanı olarak tanımlaması, diğer yönetsel disiplinlerle belge yönetimi arasındaki ilişkinin ortaya konulması ve kurumsal kalite ve verimlilik ile belge yönetimi arasında organik yakınlaşmanın kurulması, ISO 15489'un ön plana çıkan unsurları arasındadır (Chain, 2002, s.16; Stephens, 2001, s.70).

ISO 15489 genel olarak, kurumsal belge sistemlerinin tasarımı ve uygulanması, belge yönetimi çalışmalarının gerçekleştirilmesi, kontrolü, gözden geçirilmesi ve eğitimi üzerine programların, politikaların ve sorumlulukların tanımlandığı düzenlemelerden oluşmaktadır (Stepherd, 2003, s.9). Standart genel olarak iki bölümde değerlendirilmektedir. Bunlar

- ISO 15489-1: Bilgi ve Dokümantasyon-Belge Yönetimi-Bölüm1: Genel içerikli standartta yer alan unsurlar tanımlanmaktadır.
- ISO 15489-2: Bilgi ve Dokümantasyon- Belge Yönetimi- Bölüm 2: Rehber. Standarttan çok teknik rapor olmasına karşın, standardın uygulama boyutunu ortaya koymaktadır (Connelly, 2001: 26; ISO 15489-1/2 2001).

2001 yılının ilk aylarında ISO standartlar serisi içerisinde yayımlanan ISO 15489 Bilgi ve Dokümantasyon - Belge Yönetimi Standardı, yaklaşık 80 ülkenin aktif ya da pasif katılımları ve destekleri ile yayımlanmıştır. Kurumların yapısı, boyutu ve çalışma alanlarına bakmaksızın, uygulamaları gerekli görülen asgari belge yönetim unsurlarını tanımlayan standart, belge programlarının nasıl oluşturulacağı, nasıl yapılanacağı ve kontrol sistemlerinin ne şekilde organize

edileceğini ortaya koymaktadır. ISO 15489, ISO'nun geliştirdiği genel standartlar olan ISO 9000 ve ISO 14000 ile uyumlu, üzerinden kurumsal, bölgesel ve ulusal belge yönetim uygulamalarının geliştirilmesine elverişli bir yapıya sahiptir. Yaklaşık 50 yıllık süreçte ABD, Avustralya, İngiltere ve Kanada başta olmak üzere belge yönetimi alanında standartlar geliştirmeye yönelen tüm ülkeler, geliştirilen standart çerçevesinde belge işlemlerinin tanımlanması noktasında uzlaşıya varmış görülmektedirler (Connelly, 2001, s.26). Standardın geliştirilmesi aşamasında farklı düşüncelerin ortaya çıktığı ve bundan dolayı genel ifadelerin daha ağırlıklı olarak yer aldığına değinilmektedir. Örneğin Standardın oluşum aşamasında Yeni Zelanda delegelerinin, arşiv çalışmalarının da Standartta tanımlanmasını istediği, Almanya delegelerinin ise belge saklama dönemlerinin ayrıntılarıyla yer alması yönünde görüş bildirdikleri ifade edilmektedir. Ancak her ülkede belge ve arşiv çalışmalarını ve bunların bağlı olduğu yasal düzenlemelerin farklılıklar göstermesi nedeniyle, bu tür ayrıntılara standart içerisinde yer verilmediği dile getirilmektedir. (Connelly, 2001, s.27).

Standart "Genel" başlığı altında belge yönetimini tanımlanmakta ve ilgili terimlere açıklama getirilmekte, belge yönetiminin yararları, kurumsal yasa ve uygulamalarla ilişkisi vurgulamaktadır. "Politikalar ve Sorumluluklar" başlığı altında, kurumsal belge yönetimine ilişkin politikaların, düzenlemelerin ve uygulamaların tanımlanması, bunların yazılı hale getirilmesi ve belge yönetim sisteminin yazılanlar çerçevesinde yürütülmesi ve denetimi gerektiği dile getirilmektedir. Standardın 7. bölümü belge yönetim gereksinimlerine ayrılmıştır. Belge yönetimi gereksinimleri içerisinde kurumsal, yasal ve idari analizin yapılması, belge yönetimi ve belge yönetim unsurlarına yönelik gerekli dokümantasyonun, elde edilen bilgiler doğrultusunda gerçekleşmesi öngörülmektedir (ISO 15489-1, 2001, s.6). Daha sonraki bölümler, belgelerin özgünlüğü, güvenilirliği, kullanılabilirliği, bütünlüğü, sistematikliği, kapsamlılığı... v.b. üzerine kısa açıklamalara ayrılmıştır (ISO 15489-1, 2001, ss.7-8). Standardın 8.3.7. bölüm ise belge saklama ve ayıklama üzerine açıklamaları içermektedir. Açıklamalara göre kurumsal belge sistemi, belgelerin alıkonması ve ayıklanması için gerekli verileri sağlayacak, kolaylaştıracak özelliklere sahip olmalıdır. Bölümde, belgelerin alıkonması ve ayıklanması için doğru zamanlama ve etkin karar vermeye yönelik bir sistemin oluşturulması ve bu sistemin sürekliliğinin sağlanması üzerinde durulmaktadır. Yine 8.4. bölümde dile getirilen etkin belge sisteminin tasarımına yönelik ön araştırma, iş aktivitelerinin analizi, belge gereksinimlerinin tanımlanması, ve mevcut sistemin değerlendirilmesi gerektiği vurgulanmaktadır (ISO 15489-1, 2001, ss.9-10). Standardın 9.2. bölümü, belgelerin ne kadar elde bulundurulacağının saptanması üzerine açıklamaları içermektedir. Bölümde, belge sistemi içerisinde belgelerin elde bulundurulacağı süreye karar vermek için yasal koşulların değerlendirilmesi, iş ve sorumluluklara yönelik gereksinimlerin saptanması, risklerin öngörülmesi üzerinde durulmaktadır. Tüm bu çalışmalar sonucu ortaya çıkan bilgilerin, politikalara ya da standartlara dönüştürülmesi ve ilgili birimlerde uygulamaların bu çerçevede gerçekleşmesi istenmektedir. Standart bu ifadelerle son bulmaktadır (ISO 15489-1, 2001, s.11).

Geliştirilen Uluslararası Standart çerçevesinde hazırlanan Rehber ise, yukarıda dile getirilen unsurların, daha iyi anlaşılması için gerekli açıklamaları içermektedir (ISO 15489-2, 2001, ss.1-24). Bu bağlamda geliştirilen uluslararası standardın yöntem ve teknikleri uzun yıllardır kabul edilen belge yönetimi uygulamalarına yönelik geniş bir meşruiyet ortamının sağlanmasına katkı sağlayacağı ve kurumsal yönetimin vazgeçilmez bir unsuru ve çalışma alanı olarak kabul edilmesini hızlandıracağı düşünülmektedir. Böylece, kalite sistemlerine geçmeye ve kalite belgesi almaya yönelen kurumlar, uygulamaya geçirmeleri gereken belge yönetimi çalışmalarına yönelik temel bilgileri ve gereklilikleri, Standart ve Standart çerçevesinde hazırlanmış olan rehberden sağlayabileceklerdir. Standartta özetle aşağıdaki unsurlar üzerinde durulmaktadır:

a. Her bir iş süreci için belge gereksinimlerini belirleme.
b. Belge ve ilgili belge araçlarını tanımlama.
c. Gerekli üstveri unsurlarını oluşturma
d. Belge erişim ve yayımına yönelik sistemler geliştirme
e. Risk yönetimi
f. Belge korumaya yönelik unsurlar
g. Belge güvenliği
h. Belge saklamaya yönelik unsurlar (Connelly, 2001, s.28).

Elektronik veya basılı ortamda belgelerin üretiminden imhası veya arşive nakline kadar olan belge yönetimi süreçlerine bir çerçeve çizen uluslararası standarttır. Kurumların belge yönetimi sistemi kurmak veya var olan sistemlerini geliştirmek için yararlanılabilmektedir. ISO 15489'a göre (2001, s. 7) kurumlar belgelerin üretimi, sağlanması, iletilmesi, korunması ve imhası işlemlerini prosedür ve politikalara dayandırmak durumundadırlar. Belgeler, yetkili olmayan kişiler tarafından ekleme, silme, değiştirme, kullanma ve saklama işlemlerinin yapılmasına karşı korunmalıdır (Borglund ve Anderson, 2010, s. 17).

ISO 15489'a göre, özel sektör ve kamu sektöründeki iç ve dış kullanıcılar tarafından üretilen belgelerin yönetilmesine rehberlik edecek bilgiler içermektedir. ISO 15489-2 ise ISO 15489'un uygulanması için, belge yönetimi uzmanlarına ve kurumlarında belge yönetiminden sorumlu kişilere rehber niteliğindedir. Belge yönetimi ihtiyacı olan tüm kurumlar için ISO 15489 uygulanmasında bir metodoloji sağlamaktadır. ISO 15489'a uyum sağlamak isteyen kurumlara dikkat edilmesi gereken faktörler ve süreçler hakkında genel bir bakış açısı sağlayacak esasları kapsar.

Son güncellemesi 2016'da yapılan (ISO 15489-1:2016) ISO 15489 kurumların; belge yönetim sisteminin fonksiyonel özelliklerinin ve kurumun ihtiyacına yönelik belge yönetimi politikasının belirlenmesine, belgelerin tasnifine, üstverilerinin oluşturulmasına ilişkin esasları saptanmasına, belgelerin

bütünlüğüne ilişkin esasları oluşturulmasına, belgelerin depolama ve tasfiyesine ilişkin koşulların tanımlanmasına katkı sağlar. Standartta belgelerin ilk oluşumundan tasfiyesine kadar olan bütün süreçlere ilişkin koşullar tanımlanmıştır.

DoD 5015.2 (The U.S. Department of Defense's Design Criteria Standard for Electronic Records Management Software Applications; ABD Savunma Bakanlığı Elektronik Belge Yönetimi Yazılım Uygulamaları İçin Standart)

90'lı yılların başından itibaren Amerikan Savunma Bakanlığı, elektronik belge yönetimi alanında yazılımlar geliştirmeye yönelmiştir. Bu süreçte yazılım programları geliştirilirken ilgili alanda standartların eksikliğini ön plana çıkmış ve çalışmalar, yazılım uygulamaları için standart geliştirmeye yönlendirmiştir. Dod 5015.2 Elektronik Belge Yönetim Yazılım Uygulamaları İçin Standart, Amerikan Ulusal Arşivi NARA'nın katkılarıyla bu çerçevede geliştirilerek 1997 yılında yayımlanmıştır (Chain, 2002, s.16; DoD 5015.2, 2002).

Standardın geliştirilmesi süreci, 1993 yılında ABD Ulusal Arşivi NARA (National Archives and Records Administration), ABD Ordusu ve Hava Kuvvetleri ile Ordu Araştırma Laboratuarları'nın birlikte DoD Belge Yönetimi Çalışma Grubunu (Records Management Task Force) oluşturması ile başlamıştır. Standardın teorik altyapısının ve özellikle elektronik belgelerin güvenilirliği ve otantikliği üzerine yaklaşımların, British Colombia Üniversitesi ile Pittsburgh Üniversitesinde geliştirildiğine değinilmektedir (Gable, 2002, s.33). Çalışma Grubu 1995 yılında, Belge Yönetimi Uygulama Yazılımları İçin Veri Unsurları ve İşlevsel Temel Gereksinimler (Functional Baseline Requirements and Data Elements for Records Management Application Software) adlı bir rapor yayımlamıştır. Çeşitli federal kuruluşlar ile ilgili konuda yazılım üreten kurumlara gönderilen rapor, gelen öneriler ile birlikte 47 temel kriterden oluşan bugünkü konumunu almıştır (Gable, 2002, s.33).

Dod 5015.2 ABD Savunma Bakanlığı ve NARA tarafından belirlenen asgari belge ve arşiv yönetimi gereksinimlerini ortaya koymaktadır. Amerikan Savunma Bakanlığı Enformasyon Dairesi (U.S. Defense Information System Agency) tarafından geliştirilmesine karşın, tüm kurumsal yapılara uyumlu bir içerikte hazırlandığı dile getirilmektedir. Standart günümüzde pek çok kamu ve özel kurum ile uluslararası organizasyon tarafından, belge yönetim yazılımlarını sağlama aşamasında etkin olarak kullanılmaktadır (Spratt, 2004, s.6).

Standardın, yayımlandığı tarihten itibaren elektronik belge yönetimi alanında, olmazsa olmaz (de facto) olarak kabul edilmeye başlandığı, ABD Ulusal Arşivi tarafından onaylanan ve dünyada kabul gören kendi alanındaki ilk standart olduğu üzerinde durulmaktadır. Özel sektör ya da kamu kesiminde belge yönetimi yazılımları alınırken, Standartta belirtilen unsurların temel alındığına

değinilmektedir. Yine İngiliz Ulusal Arşivi (British Public Records Office) ve Avrupa Birliği tarafından geliştirilen MoReq'in (Model Requirements for Electronic Records Management; Elektronik Belge Yönetimi Model Gereksinimi) ortaya koyduğu elektronik belge yönetim rehberi ve modellerinin, DoD 5015.2 temel alınarak geliştirildiği belirtilmektedir. (Gable, 2002, s.32). Standart, özellikle elektronik belge yönetim yazılım uygulamalarının tasarım aşamasında, uyulması gereken kriterleri ortaya koyması bakımından oldukça önemli görülmektedir (Archives and Records Assocaition of New Zelland, 2004, s.1). DoD 5015.2 kodu ile 57 sayfa olarak yayımlanan Standart. ABD dışında İngiltere ve diğer bazı ülkelerce de kabul edilmiştir (Dod 5015.2, 2002; Stephens, 2001, s.70).

DoD 5015.2 standardı içerisinde yer alan tanımlar ve gereksinimler 2002 yılında gözden geçirilmiş ve çeşitli eklemeler yapılmıştır. Standart içerisinde yer alan ve Standardın II. Bölümünü oluşturan, belge yönetimi uygulamaları için gerekli unsurlar aşağıda tablo 1'de verilmektedir. Standartta ayrıca giriş ve tanımlama bölümü olan I. Bölümün ardından, III. Bölüm zorunlu olmayan unsurlara, IV. Bölüm de 'Sınıflanmış Belge Yönetim' altında uygulamalara ayrılmıştır (Dod 5015.2, 2002).

Tablo 1. Dod 5015.2 İçerisindeki Zorunlu Gereklilikler

DoD 5015.2		**Gereklilikler**	**Alt Bölüm Sayısı**
C.2.1	1	Depolama ortamına bakılmaksızın tüm belgelerin aynı sistem içerisinde tanımlanması	0
	2	Dört basamaklı tarihlemeye göre yerleşim	0
	3	Tanımlanmış kullanıcı ve değişiklik alanları oluşturma	0
	4	Önceki uygulamalarla sisteme uyumunu sağlama	0
	5	İlgili yasal düzenlemelerle uygulamaların karşılaştırılması	0
C.2.2	1	Dosya planlarının uygulanması-Standart dosya planı ve gerekli belge dosya unsurlarını belirlenmesi	6
	2	Belge şemaları geliştirme	7
	3	Bildirim (declaring) ve dosyalama belgeleri- standartlar ve gerekli üstveri unsurlarının belirlenmesi	26
	4	Elektronik posta	3
	5	Belge depolama	4
	6.1	Belge gözden geçirme (screening) 'Yaşam döngüsü'	6
	6.2.	Belge dosyalarının kapanması (closing) 'Yaşam Döngüsü'	2
	6.3.	Belge dosyalarının işleminin sona ermesi (cutting off) 'Yaşam Döngüsü'	2
	6.4.	Belge dosyalarının dondurulması (freezing) ve tekrar açılması (unfreezing) 'Yaşam Döngüsü'	4
	6.5.	Belge transferi 'Yaşam Döngüsü'	5
	6.6.	Belgelerin imhası 'Yaşam Döngüsü'	6
	6.7	Hayatı belge döngüsü (Cycling Vital Records)	4
	6.8.	Belge araştırma ve belge erişim	9
	7	Erişim kontrolü	5
	8	Sistem denetimi	6
	9	Sistem yönetimi	6

(Dod 5015.2, 2002; Gable, 2002, 34).

DoD 5015.2 elektronik belgelerin yönetimi için gerekli unsurları tanımlıyorsa da, her kurumsal yapının kendi gereksinimleri doğrultusunda bir belge akış ve buna bağlı belge sistemini oluşturması gerekmektedir. Kurumsal olarak üretilen ya da sağlanan dokümanların hangilerine, ne aşamada belge statüsünün verileceğinin belirlenmesi de doğrudan o kuruma yönelik yapılacak analizlerin sonucunda ortaya konulabilmektedir. Yukarda sıralanan tüm unsurlar, belge statüsü kazanmış dokümanlara yönelik, önceden belirlenmiş zaman aralıklarında yapılması gereken işlemleri ortaya koymaktadır.

DoD 5015.2'nin 3. bölümde ortaya konulan zorunlu olmayan uygulamalar ise aşağıda Tablo 2'de verilmektedir.

Tablo 2. Dod 5015.2 İçerisindeki Zorunlu Olmayan Gereklilikler

DoD 5015.2 Sayısı	**Zorunlu Olmayan Gereklilikler**		**Alt Bölüm**
C.3.1 Zorunlu Olmayan Uygulamalar	1.	Depolama olanakları	
	2	Dokümantasyon	
	3	Sistem performansı	
	4	Donanım özellikleri	
	5	Sistem olanakları	
	6	Ağ olanakları	
	7	Protokoller	
	8	Elektronik posta ara yüzleri	
	9	Son kullanıcı oryantasyonu ve eğitimi	
C.3.2 Diğer Yararlı Özellikler	1	Küresel değişimler	
	2	Yığın (bulk) yükleme kapasitesi 'Dosyalama ön çalışmaları, elektronik belgeler ve üstveri unsurları için'	
	3	Diğer yazılım uygulamaları için ara yüzler	
	4	Rapor yazma kapasitesi	
	5	On-line yardım	
	6	Doküman görüntüleme araçları	
	7	Faks entegrasyon araçları	
	8	Bar kod sistemleri (elektronik olmayan belgeler için)	
	9	Erişim asistanı (örneğin tam metin taranması gibi)	
	10	Dosya planı unsurlarının seçimi/tarama kapasitesi	
	11	İş akışı ve veya doküman yönetim özellikleri	
	12	Belge yönetim formları ve diğer formlar	
	13	Yazılı etiketler (printed label)	
	14	Görüntüleyici (viewer)	
	15	Web kapasitesi	
	16	Kamu bilgi yerleşim sitemi (government information locator service)	
	17	Off-line belgeler için geliştirilmiş destek	

(Dod 5015.2, 2002; Gable, 2002,34).

TS 13298 Bilgi ve Dokümantasyon - Elektronik Belge Yönetimi Standardı

TS 13298 standardı Türk Standartları Enstitüsü tarafından yayımlanmış. Türkiye'ye ait bir standart olmakla birlikte kapsamı ve içeriği göz önünde bulundurularak uluslararası standartlar içerisinde verilme gereği hissedilmiştir. TS 13298 kurumlarda üretilen elektronik belgelerin belge niteliklerini koruyabilmeleri için uyulması gereken kuralları belirlemektedir. Standardın amacı; elektronik belge yönetimi yazılım uygulamalarında kamu yönetimi ve belge diplomatiğine uygun olarak belge yönetimi sistemlerinin tüm unsurlarını belirlemek, basılı belgelerin dijitalleştirilmesi ve dijital arşiv yönetim sistemlerini tanımlamaktır. Standart, kurumlarda üretilen ve/veya üretilmesi muhtemel elektronik dokümanların belge niteliğinin korunabilmesi için gerekli standartların belirlenmesi amacıyla aşağıdaki konuları kapsamaktadır:

- Elektronik belge yönetimi sistemi (EBYS) için gerekli sistem gereksinimleri,
- EBYS için gerekli belge yönetim teknikleri ve uygulamaları,
- Elektronik belgelerin yönetilebilmesi için gerekli gereksinimler,
- Elektronik ortamda üretilmemiş belgelerin yönetim fonksiyonlarının elektronik ortamda yürütülebilmesi için gerekli gereksinimler,
- Elektronik belgelerde bulunması gereken diplomatik özellikler,
- Elektronik belgelerin hukuki geçerliliklerinin sağlanması için alınması gereken önlemler,
- Güvenli elektronik imza ve mühür sistemlerinin uygulanması için gerekli sistem alt yapısının tanımlanması (TS 13298, 2015).

ISO 23081 - Bilgi ve Dokümantasyon - Belge Yönetimi Üstveri Standardı

ISO 15489 çerçevesinde belgeleri yönetirken ihtiyaç duyulan üstverileri tanımlama, uygulama ve kullanmaya yönelik bir üstveri standardıdır. Bir belge üstverisi oluştururken veya üstverileri değerlendirme ihtiyacında yararlanılabilmektedir. ISO 15489'da belirtilen belgelerin doğruluğu, güvenilirliği, bütünlüğü ve kullanılabilirliğini sağlamak için üstveriler oluşturulmak durumundadır (Borglund & Anderson, 2010, s. 18). ISO 23081 üç bölümden oluşmaktadır. Bunlar:

- İlkeler
- Kavramsal sorunlar ve uygulama sorunları,
- Kendi kendini değerlendirme yöntemleridir

Bir dokümanı belge yapan, kanıt niteliği taşımasına sağlayan, doğruluğunu ve güvenilirliğini tanımlayan bilgiler, tanımlama bilgisinde bir diğer deyişle üstveri bilgisinde yer alır.ISO 23081'in 2006 versiyonunda belge yönetiminin süreçleri, belge yönetimi sistemleri tanımlanmakta, üstverinin nasıl yapılandırılacağı

anlatılmaktadır. 2009'da yayınlanan versiyonunda ise farklı sistemler arasında birlikte çalışabilirliği sağlamaya dönük yeni bir bölüm eklenmiştir. Standardın bir diğer hedefi de belgelerin farklı sistemler üzerinde gelecekte de kullanılabilirliğini sağlamaktır.

ISO 23081'ye göre üstveri 6 bileşenden oluşur. Bunlar

1. Belgenin kendisi hakkında üstveri
2. kurallar ve politikalar hakkında üstveri,
3. Yetkiler hakkında üstveri,
4. İş süreçleri hakkında üstver,
5. Belge yönetim süreçleri hakkında üstveri,
6. Üstveri belgesi hakkında üstveri (Borglund ve Anderson, 2010, s. 19).

Belgenin kendisi hakkında üstveriler belgenin hangi formatta olduğu, ne zaman ve kim tarafından üretildiği gibi bilgileri içermektedir. En önemli üstderilerden biridir. Belgeyi tanıtmak için kullanılan üstveri alanlarıdır. Belgeler kurumun politikalarına uygun olmak zorundadır. Kurallar ve politikalar hakkında üstveri alanı olmazsa belgenin kurum ile olan bütünlüğü, belgenin doğruluğu ve güvenilirliğinden emin olmak söz konusu değildir. Belgeye erişim sağlayabilecek yetkili kişiler, değişiklik yapmaya, silmeye, saklamaya yetkili kişiler ve belge hakkında bilgi alabilecek kişiler üstveri alanlarında belirtilmelidir.

ISO 2308'de ayrıca üstveriyi açıklayan 6 tür ve 4 varlık (entity) yer alan almaktadır. Tür alanı içerisinde; kimlik, tanımlama, kullanım, olay planı, olay tarihi ve ilişki yer almaktadır. Varlık altında ise; insanlar, belge, iş ve yetkiler yer almaktadır (Niu, 2013, s. 7). Üstveri sadece bilgi erişimi değil, bilgi güvenliği, teknik koşulları, bilgi kaynakları ve belgelerin yaşam döngüsündeki aşamalarını, gizlilik ve erişim kısıtlamalarını belirleyen bir konudur.. Üretilen kaynaklar ne olursa olsun üstveri yönetim politikaları yetersizse erişim, yönetimi koruma ve güvenlik politikaları bundan olumsuz olarak etkilenecektir. Bu kapsamda özellikle EBYS sistemlerinde üstveri uygulamalarının çok yönlü değerlendirmelere dayanılarak geliştirilmesi gerekmektedir. ISO 23081, ts 13298 gibi kurumsal bilgi ve belge yönetimi sistemlerinde üstveri unsurlarının geliştirilmesinde referans alınması gereken bir düzenlemedir.

Kurumsal Belge Yönetimi Sistemlerinin Geliştirilmesinde Yararlanılabilecek Standartlar

ISO 16175-1/2: Principles and functional requirements for records in electronic office environments (elektronik çalışma ortamında hazırlanan belgeler için prensipler ve fonksiyonel gereklilikler), (TC-46), (2010)

ISO 16175 standardının amaçları arasında kurumlarda belgelerin daha iyi yönetilmesini, kurumlarda faaliyetlerin etkinliğini arttırarak işletme ihtiyaçlarını desteklemesi, belgelerin otomatik olarak saklanması dolayısıyla kontrolün kolay yapılmasına imkân sağlanması, verilerin korunmasına yönelik önlemlerin

alınması, kayıtların iyi yönetilmesi dolayısıyla hesap verilebilirlik ve şeffaflık konularında işletmeye katkıda bulunulması, yazılım üreticilerine dijital belgelerin arşivlenmesi ve yazılımların işlevsel özellikleri konusunda referans teşkil ederek, aynı dili konuşan yazılımların oluşturulması yer almaktadır.

ISO 13008: Digital records conversion and migration process (Dijital Belgelerin Dönüşümü ve Taşınması) (TC-46), (2012)

ISO 13008 standardının amaçları arasında; teknolojik gelişmeler sonucunda dijital belgelerin bir formattan başka bir formata dönüştürme esaslarını belirlemek, dönüşümler sırasında karşılaşılabilecek sorunlara çözümler sunmak, dönüşüm için kullanılabilecek metotları belirlemek, belirli bir sistem üzerinde yüklü evrakların başka sistemlere aktarım esaslarını belirlemek yer almaktadır.

ISO TR 26122: Work process analysis for records (Belge işlemleri analizi) (TC-46), 2008

ISO/TR 26122 standardının amaçları arasında; belgelerin kurum içerisinde hiyerarşik dolaşımını belirlemek, kurum faaliyetleri doğrultusunda evrakın akışını düzenlemek, kurum belge süreçlerinin analizi ve gerekli kuralların belirlenmesi, kurum faaliyetleri ile üretilen evraklar arasındaki ilişkinin düzenlenmesi yer almaktadır.

ISO 30300-30304: Management systems for records (Belge Yönetim Sistemleri), (TC-46), (2011)

ISO 30300 Standardının amaçları arasında; belge yönetim sistemlerinin uygulama aşamasından ziyade genel çalışma prensiplerini belirlemek, belge yönetim sistemlerinin kurumun ana yönetim sistemi ile entegrasyonuna ilişkin esasları belirlemek, belge yönetim sisteminin ihtiyaçlar doğrultusunda sürekli gelişimi için gerekli kontrol esaslarını belirlemek, bir birim tarafından belge yönetim sistemlerinin sertifikasyonunu sağlamak, belge yönetim politikasının belirlenmesi, değerlendirilmesi ve iyileştirilmesine ilişkin esasların belirlenmek yer almaktadır (Şahin, 2016).

Uluslararası Arşiv Konseyinin (International Council on Archives, ICA) Elektronik Belge Yönetimiyle İlgili Çalışmaları

Uluslararası Arşiv Konseyi milli arşiv düzeyinde yaklaşık olarak 195 ülkeden 1500 üyeye sahiptir ICA bünyesinde yer alan Mesleki Standartlar ve İyi Uygulama örnekleri Komitesi (Committee on Best Practices and Professional Standards (CBPS) belge yönetimi alanında standartlaşmaya yönelik aşağıdaki standartları geliştirmiştir (ICA, 2009; Eroğlu, 2013):

- CBPS - Progress report for revising and harmonising ICA descriptive standards
- CBPS - Relationship in archival descriptive systems
- eArchiving Digital Record Exchange Standard Jurisdictional Survey
- Business Requirements Specification
- ICA-Req
- ISAAR (CPF): International Standard Archival Authority Record for Corporate Bodies, Persons and Families
- ISDIAH: International Standard for Describing Institutions with Archival Holdings
- ISDF: International Standard for Describing Functions
- ISAD(G): General International Standard Archival Description - Second edition (ICA,

Kurumsal Bilgi Sistemleri ve Bilgi Hizmetlerine İlişkin

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı

Kurumlarda bilginin korunması, bilgiye yalnızca yetkili kişilerin erişiminin sağlanması ve yetkililere ihtiyaç duyulduğunda doğru ve güvenilir bilginin ulaştırılması için uyulması gereken kuralları belirleyen uluslararası bir standarttır.

ISO 14721 Açık Erişim Bilgi Sistemleri Standardı (Open Access Information Systems Standard; OAIS)

ISO 14721 Consultative Committee for Space Data Systems (CCSDS) tarafından geliştirilmiştir. ISO 14721 standardı açık ve kurumsal arşiv için gerekli olan bilgi sistemine yönelik olarak bir referans modeli geliştirmiştir (OAIS, 2008).

ISO 25577:2008: Bilgilendirme ve Dokümantasyon – MarcXchange

ISO 25577:2008 Diğer üstveri çeşitleri gibi bibliyografik kayıtlar için XML tabanlı genellenmiş gereksinimleri belirtir. ISO 25577:2008 veri işleme sistemleri arasında iletişim için tasarlanmış öncelikli bir ana çerçeve, fakat sistemler içinde işleme biçimleri ile ilgili de kullanılabilen genellenmiş bir yapıyı tanımlar.

MarcXchange' in potansiyel kullanımları:

- Tüm MARC kayıtlarını ya da bir grup MARC kaydını XML 'de anlatmak için

- XML sözdiziminde orijinal kaynak tanımlaması için
- Metadata Kodlama ve İletim Standartı için genişletilmiş şema olarak
- Marc kayıtlarını XML kayıtlarına çevirmek için
- Yayıncı iletim bilgileri için
- Geçici bir format olarak her çeşit bilginin değiştirilmesi ya da dönüştürülmesi aracı olarak örneğin: dönüşüm, yayın, düzenleme, onaylama
- Elektronik kaynakla paketlenmiş üstveri için kullanılabilir.

TS 12115 Yangın Önleme - Kütüphane ve Arşivlerde

Bu standart, müstakil veya bir yapının bölümü olarak kullanılan kütüphane ve arşivde meydana gelecek yangına karşı önceden alınacak önlemlerle ilgili kuralları kapsar.

TS ISO 11108 Bilgi ve Dokümantasyon-Arşivlik Kağıt-Kalıcılık ve Dayanıklılık Özellikleri

Bu standart arşivlik kağıt özelliklerini , dayanıklılık ile ilgili koşullarını tanımlayan bir standarttır. Referans aldığı standartlar arasında BS ISO 11108-EQV; ISO 11108 –EQV yer almaktadır. Ayrıca standartta TS 635 ISO 186 :1996; TS 636 EN 20187 :1996; TS ISO 302 :2001; TS 3122 EN ISO 536 :1998; TS 4423 EN 21974 :1996; TS ISO 4046 :1996; TS 5162 ISO 5626 :1997; TS 4842 :1986; TS EN ISO 9706 :1999; TS ISO 10716 :2002 standartlarına atıflar yapılmaktadır.

TS ISO 6357 Dokümantasyon - Kitap ve Diğer Yayınların Sırt Başlıkları.

Bu standart, raflarda bulundurulacak kitap, seri halindeki yayınlar, süreli yayınlar, raporlar ve kasa, kaset gibi dokümantasyon ve bunlara benzer diğer eşya ile ilgili sırt başlıkları ve karşılık gelen metinlerin genel yerleşimi (konum ve yön) ve kullanım kurallarını kapsar. Bu standart, yalnız Latin, Grek ve Kril alfabeli metinlere uygulanır.

TS 2143/ ISO 2108 Bilgi ve Dokümantasyon–Uluslararası Standard Kitap Numaralandırılması

Bu standardın amacı, her bir uluslararası standart kitap numarasının belirli bir yayınevi tarafından yayınlanan bir kitabın veya diğer monografik yayınların ad veya baskısına karşılık gelecek şekilde tekleştirilmesine yönelik numaraların belirlenmesi işini, düzenlemek ve standartlaştırmaktır.

TS 12567 Formlar- Yayın Ödünç Verme Fişi- Kütüphanelerde Kullanılan

Bu standart kütüphanelerdeki yayınların kütüphane içinde veya kütüphane dışına okuyucuya verilmesini sağlamak amacıyla kullanılan yayın ödünç verme fişini kapsar.

ISO 11620:2008 Bilgi ve Dokümantasyon: Kütüphane Performans Göstergeleri (Information and documentation -- Library performance indicators)

ISO 11620 uluslararası bir standart olarak kütüphaneler için performans göstergesi gereksinimlerini belirlemek ve tüm kütüphane türleri için bir dizi performans göstergesi oluşturmak için geliştirilmiştir. Bu standart ayrıca performans göstergeleri kullanılmayan kütüphanelerde performans göstergelerinin nasıl uygulanabileceği konusunda da rehberlik yapmayı da amaçlamaktadır. Standart performans göstergelerinin kısa tanımlarına yer vermekte, farklı gruplar altında performans faktörlerini tanımlamaktadır. Ayrıca standart, bilgi merkezlerinde koleksiyonun, kullanıcılar ve çevresel koşullarla ilgili ihtiyaç duyulan bilginin analizine, performans göstergelerinin uygulanmasına ilişkin ayrıntılar içermektedir. Standart uluslararası koşullarda tüm kütüphane türlerine uygulanabilecek biçimde hazırlanmıştır. Performans göstergesinin uygulanmasındaki sınırlamalar her performans göstergesi için EK-B'de listelenmiştir. Bu uluslararası standardın temel amacı performans göstergelerinin kütüphanelerde kullanımını desteklemek ve performans ölçümünün nasıl yürütüleceği hakkında bilgiyi yaymaktadır. Elektronik hizmetler gelişmeye ve değişiklikten geçirmeye devam edileceği bu uluslararası standarttaki performans göstergeleri ile ilgili böyle bir değişim/gelişim kontrol edilmektedir. Standartta kütüphane performans göstergeleri kaynaklar, erişim, alt yapı; kullanım; verimlilik; olanaklar ve gelişme olmak üzere dört ana performans göstergesinden oluşmaktadır. Bu dört ana performans göstergesi koleksiyon, erişim, olanaklar, personel gibi alt göstergelerden oluşmaktadır. Alt performans göstergeleri de kendi içinde alt başlıklar halinde belirtilmiştir. Bu uluslararası standartta her bir performans göstergesinin ve alt performans göstergelerinin;

- amacı
- kapsamı
- performans göstergesinin tanımı
- yöntemi

- performans göstergesini etkileyen faktörler ve bu faktörlerin yorumlanması
- kaynaklar
- ilişkili olduğu performans göstergesi ayrı ayrı verilmektedir.

Bilgi Sistemleri İle İlişkili Standartlar

ISO'nun kurumsal bilgi sistemlerinin geliştirilmesinde değerlendirilebilecek standartları aşağıda sadece başlıklarıyla verilmektedir.

- ISO/IEC 11179 Information technology — Metadata registries (MDR) Bilgi Teknolojisi Veri Elemanlarının Özellikleri ve Standardizasyonu (CISN, 2013; ISO, 2004).
- ISO/TR 18492:Document management-long-term preservation of electronic document-based information- Technical Report (Elektronik dokümana dayalı belgelerin uzun süre korunması- Teknik rapor)
- ISO 19005-1:Document management-electronic document file format for long-term preservation-Part 1: Use of PDF 1.4 (PDF/A-1) (Doküman yönetimi-uzun süreli koruma için elektronik doküman dosya biçimi-Bölüm 1: PDF kullanımı 1.4 2.5.1.2.5.
- ISO 22310: Information and documentation-Guidelines for stating records management requirements in standards (Enformasyon ve dokümantasyon-İlişkili Standartlardan Belge Yönetim Gereksinimlerini Karşılamak için Kılavuz)
- ISO Technical Report 20943-1, Information Technology- Procedures for Achieving Metadata Registry (MDR) ContentConsistency – Part 1: Data Elements, Bilgi teknolojisi - meta kayıt içerik tutarlılığı sağlamak için prosedürler
- ISO/IEC 17799, Information Technology- Security Techniques- Code of Practice: Bilgi güvenliği yönetimi

METS - Üstveri Kodlama ve İletim Standardı (Metadata Encoding and Transmission Standards)

2001 yılında Dijital Kütüphane Federasyonu (Digital Library Federation) sponsorluğunda oluşturulmuş bir yapıdır. Metadatanın kodlanması ve aktarımına yönelik bir standarttır. Aynı zamanda bir çatı olarak da görev taşımaktadır. Sürekliliğini ve yaşatımını Library of Congress sağlamaktadır. Standart açık ve kurumsal arşivlerde içeriğin XML ile ifade edilmesini, dolayısıyla elektronik yayıncılığı destekleyen bir yapıya sahiptir. METS standart ve bir çatı olarak kurumsal arşivler, kütüphaneler ve müzelerin içeriklerini elektronik ortamda sunabilmeleri için son derece önemlidir (METS Primer Reference Manual, 2007).

Sanatçılar, yazarlar, müzisyenler, kamu çalışanları, politikacılar, bilim adamları ve genel olarak halk günlük yaşamlarında giderek daha fazla oranda elektronik sistemlerde bu belgelerle çalışmakta ve işlerini bu belgeler üzerinden yürütmektedirler (Duranti ve Rogers, 2011, s.384).

METS (Metadata Encoding and Transfering Standard, Üstveri Kodlama ve Transfer Standardı) profilleri ortak karakterlerin paylaşıldığı dijital obje sınıflarını tanımlamaktadır. Örneğin içerik dosya formatları (dijital imajlar, TEI metinleri) ya da üstveri kodlama formatları (DODS ya da Dublin Core) bu kapsamda yer almaktadır. Profillerin, METS programcılarının objeleri en azından zorunlu tutulan alanlarda tanımlayabileceği düzeyde bilgiyi içermesi gerekmektedir. METS profilleri XML formatında METS XML Profil Şemasını uygun olarak hazırlanmak durumundadır (CDL Guidelines for Digital Objects, 2011, s.3-5).

Bu kapsamda tanımsal üstveri kaynakların içerik özelliklerinin ifade edilmesi için kullanılmaktadır. Analog ortamdan dijital ortama aktarılan içeriğin tanımsal üstverileri analog ortamdaki tanımlama özelliklerinden alınabilmektedir. Örneğin üretici (creator) bilgisi MARC'da yazar alanından, resimleyen ya da yayımcıdan alınabilmektedir. Bazı durumlarda analog içeriğin tanımlamaları ile dijital tanımlama elemanları tam olarak örtüşmeyebilmektedir. Bu durumda:

- Tanımlama üstveri elemanlarının kullanımında standart bir yapı kullanılması önerilmektedir. Bu yapı tüm kaynakların tanımlanmasında aynı biçimde uygulanmalıdır.
- Elemanların belirlenmesinde kullanıcıların en kolay erişim sağlayabileceği alanlar göz önünde tutulmalıdır (CDL Guidelines for Digital Objects, 2011, s.11-12).

Aşağıda örnek bir üstveri etiketleme alanları şema gösterimi yer almaktadır.

Eleman	**Statü**
Tanımlayıcı (Identifier) Kod	Gerekli eleman
Başlı (Title)	Gerekli eleman
Üretici (Creator)	Gerekli elaman (Not: Eğer hiçbir isim sağlanamazsa, iştirakçi, organizasyon, arşiv, yayımcı bilgisi kullanılabilir)
Tarih (Date)	Gerekli eleman
Tanımlama (Description)	Önerilen eleman
Dil (Language)	Önerilen eleman
Konu (Ad) (Subject-name)	Önerilen eleman
Konu (Başlık) (Subject-Title)	Önerilen eleman
Konu (Yer) (Subject-place)	Önerilen eleman
Konu (Tema, fonksiyon, iş) (Subject-topic, function ya da occupation)	Önerilen eleman
Tür (Genre)	Önerilen eleman
Tür (Type)	Gerekli eleman

Format/fiziksel tanımlama (Format/physical description)	Önerilen eleman
İlişkili koleksiyon/proje (Related collection/Project	Önerilen eleman
Organizasyon/Arşiv (Institution/repository)	Gerekli eleman
Katkı sağlayan (Contributor)	Önerilen eleman
Yayımcı (Publisher)	Önerilen eleman

Elektronik bilgi sistemlerinde METSRights or PREMIS kullanarak haklarla ilgili bilgiler sağlanma önerilmektedir.

Tablo 3. Haklar Yönetimi İdari Üstveri Etiket Alanları Şema Gösterimi

Eleman	**Statü**
Telif hakları statüleri (Copyright status)	Tavsiye edilen eleman
Telif hakları açıklaması (Copyright statemen)	Tavsiye edilen eleman
Telif hakkı tarihi (Copyright date)	Tavsiye edilen eleman
Telif hakkı sahibinin adı (Copyright owner name)	Tavsiye edilen eleman
Telif hakkı sahibinin bağlantı adresi (Copyright owner contact information)	Tavsiye edilen eleman

(CDL Guidelines for Digital Objects, 2011, s.13-16).

Kültürel Miras Kapsamındaki İçeriğin Tanımlamasına İlişkin Standartları

Kodlanmış Arşivsel Tanımlama (EAD) ve ISAD (G), MARC 21 Standartları

Kodlanmış Arşivsel Tanımlama (Encoded Archival Description, EAD) standardı, 1993 yılında ABD'nin Berkeley şehrinde bulunan California Üniversitesi'nde bir proje kapsamında geliştirilmişi. Arşiv kaynaklarının tanımları için standart geliştirilen standartta 170'in üzerinde etiket alanı belenmiştir. EAD aşağıdaki başlıklardan oluşmaktadır:

- Başlık
- Geniş tarih aralığı
- Dar tarih aralığı
- Kimlik Numarası

Tablo 4. ISAD(G) ve EAD Tanımlama Alanlarının Karşılaştırılması

ISAD(G)	EAD
3.1.1 Referans kodları	<eadid> Ülke Kodu ve Ana Ajans Kodu nitelikleri ile <unitid> Ülke Kodu ve Arşiv Kodu nitelikleri ile
3.1.2 Başlık	<unittitle>
3.1.3 Tarihler	<unitdate>
3.1.4 Seviyelerin tanımlanması	<archdesc> ve <c> Seviye niteliği
3.1.5 Kapsam ve biriminin ortası	<physdesc> ve alt ögeleri <extent>, <dimensions>, <genreform>, <physfacet>
3.2.1 Yaratıcının ismi	<origination>
3.2.2 İdari / Biyografik tarih	<bioghist>
3.2.3 Arşiv geçmişi	<custodhist>
3.2.4 Hızlı bilgi edinme	<acqinfo>
3.3.1 Kapsam ve içerik	<scopecontent>
3.3.2 Değerleme, yıkım ve zamanlama	<appraisal>
3.3.3 Tahakkuklar	<accruals>
3.3.4 Sistemin düzenlenmesi	<arrangement>
3.4.1Erişimi düzenleyen koşullar	<accessrestrict>
3.4.2 Kullanma koşulları	<userestrict>
3.4.3 Dil / komut materyali	<langmaterial>
3.4.4 Fiziksel özellikler ve teknik gereksinimler	<phystech>
3.4.5 Bulma yardımcıları	<otherfindaid>
3.5.1 Varlık ve orijinal yeri	<originalsloc>
3.5.2 Varlık ve kopya yeri	<altformavail>
3.5.3 İlgili birimlerin açıklaması	<relatedmaterial> <separatedmaterial>
3.5.4 Yayın notu	<bibliography>
3.6.1 Not	<odd> <note>
3.7.1 Arşivcinin notu	<processinfo>
3.7.2 Kurallar ve sözleşmeler	<descrules>
3.7.3 Tarih (ler) açıklamaları	<processinfo><p><date>

ISAD(G) ve EAD'de Tanımlama Alanları

Benzer biçimde Uluslararası Arşiv Konseyince (ICA) geliştirilen ISAD(G) ve arşiv kaynaklarının bibliyografik tanımlamalarını oluşturmak için geliştirilen MARC21 standartları da benzeyen bir yapıya sahiptir. İlgili standartlar sadece arşivler için değil müze, kütüphane ve el yazmaları arşivlerini listelemek ve tanımlamak amacıyla da kullanılabilmektedir. Aşağıda bu 3 standardın genel tanımlama başlıkları karşılaştırmaları olarak verilmektedir.

- Yaratıcısı
- Fiziksel Büyüklük
- Dil/Diller
- Bulunduğu yer
- Özet içerik
- Atıf ve sık kullanılan linki
- LC katalog linki
- Kapsam ve İçerik Notu
- Düzenleme Şekli
- İçerik Listesi
- İndeks Terimleri
- Koleksiyon kullanım hakları
- Basım / yükleme / paylaşım
  - Tam metin , Pdf format
  - Tam metin, Xml fomat
  - Tam metin, METS Objesi

Tablo 5. MARC 21 ile EAD Tanımlama Alanları

MARC 21	**EAD**
041 Dil	Dil kodunun niteliği <language>
100 Temel giriş – Kişi adı	<origination><persname> <origination><famname>
110 Temel giriş – Kurum adı	<origination><corpname>
111 Ana giriş - Toplantı adı	<origination><corpname>
130 Temel giriş – Tek Başlık	<unittitle>
240 Düzgün başlık	<controlaccess><title>
245 Başlık deyimi	<unittitle>
245 $ f Başlık deyimi / kapsayıcı tarihleri	<unitdate type="inclusive">
245 $ g Başlık beyanı / toplu tarihleri	<unitdate type="bulk">
254 Müzikal sunum bildirimi	<materialspec>
255 Kartoğrafik matematiksel veriler	<materialspec>
256 Bilgisayar dosyası özellikleri	<materialspec>
260 $ c Tarih	<unitdate>
300 Fiziksel açıklama	<physdesc> ve alt ögeleri <extent>, <dimensions>, <genreform>, <physfacet>
340 Fiziksel ortam	<phystech>
351 Organizasyon ve düzenleme	<arrangement>
351 $ Hiyerarşik düzen	<archdesc> LEVEL attribute
355 Güvenlik sınıflandırması kontrolü	<legalstatus>
500 Genel not	<odd> <note>
506 Erişim notu kısıtlamaları	<accessrestrict> <legalstatus>
510 Atıflar / referanslar	<bibliography>

520 Özet vs.	<scopecontent>
524 Tanımlanan malzemelerin atıfı	<prefercite>
530 Mevcut fiziksel form	<altformavail>
535 Orijinal Yer	<originalsloc>
536 Finansman bilgisi	<sponsor>
538 Sistem Detayları	<phystech>
540 Kullanma ve çoğaltmayı sağlayan şartlar	<userestrict>
541 Yeni gelen kaynak	<acqinfo>
544 Diğer arşiv malzemelerinin yeri	<relatedmaterial> <separatedmaterial>
545 Biyografik ya da tarihsel veriler	<bioghist>
546 Dil	<langmaterial>
555 Kümülatif indeks / bulma yardımları	<otherfindaid>.
561 Mülkiyet ve gözaltı tarihi	<custodhist>
581 Tanımlanan materyaller hakkında yayınlar	<bibliography>
583 Eylem	<appraisal> <processinfo>
584 Birikim ve kullanım sıklığı	<accruals>
600 Konu - kişisel ad	<controlaccess><persname role="subject"> <controlaccess><famname role="subject">
610 Konu-kurumsal isim	<controlaccess><corpname role="subject">
611 Konu-toplantı	<controlaccess><corpname role="subject">
630 Konu-tek başlık	<controlaccess><title role="subject">
650 Konu- güncel	<controlaccess><subject>
651 Konu-coğrafi isim	<controlaccess><geogname role="subject">
655 Tür / formu	<controlaccess><genreform>
656 Erişim kontrolü	<controlaccess><occupation>
657 Fonksiyon	<controlaccess><function>
69x Yerel konu erişim	<controlaccess><subject source="local">
700 Ek giriş - Kişisel ad	<controlaccess><persname> <controlaccess><famname>
710 Ek giriş - Kurumsal isim	<controlaccess><corpname>
711 Ek giriş - Toplantı adı	<controlaccess><corpname>
720 Ek giriş - Kontrolsüz	<name>
730 Ek giriş- Tek başlık	<controlaccess><title>
740 Ek giriş – İlgili ana başlık	<title>
752 Ek giriş- Hiyerarşik yer adı	<geogname>
852 Yer	<repository> <physloc>

El Yazmalarının Tanımlanması Standardı: TEİ (Text Encoding Initiative, Metin Kodlama Girişimi)

TEİ (Text Encoding Initiative, Metin Kodlama Girişimi) el yazması koleksiyonlarının tanımlanmasında yaygın olarak kullanılmaktadır. Bu çerçevede TEI'yi aktif olarak kullanan kurumlar arasında;

- Chicago Üniversitesi Kütüphanesi,
- Bodleian Üniversitesi Kütüphanesi,
- Oxford Üniversitesi Kütüphanesi,
- Uppsala Üniversitesi Kütüphanesi,
- Kolombiya Üniversitesi Kütüphanesi,
- Kaliforniya Dijital Kütüphanesi yer almaktadır.

TEİ el yazmalarının tanımlanmasına dönük kapsamlı bir içerik sunmaktadır. Bu aksamda hazırlanan doküman aşağıdaki başlıklarda ayrıntılı tanımlamalara sahiptir:

- El yazması tanımlama
- El yazması açıklama elemanları
- Deyim –seviye elemanları
- El yazması tanımlama elemanları
- El yazması başlık
- Entelektüel içerik
- Fiziksel Tanımlama
- Tarih
- Ek bilgiler
- El yazması parçaları

TEI içerisinde el yazması tanımlama elemanları aşağıdaki temel başlıklardan oluşmaktadır.

- <msIdentifier > (manuscript identifier) : Tarif edilen el yazmasını tanımlamak için gerekli bilgileri içerir.
- <head> (heading) : Başlığın her türünü içerir; örneğin bir bölümün başlığı, ya da bir liste, sözlük ve el yazmasının başlığı.
- <msContents> (manuscript contents) : Paragrafların bir dizi olarak veya yapılandırılmış el yazması öğelerini bir dizi olarak ya bir el yazması ya da el yazması kısmının entelektüel içeriği açıklar.
- <physDesc> (physical description) : Bir el yazması veya el yazması kısmının tam fiziksel açıklamasını içerir, isteğe bağlı olarak

model.physDescPart sınıfından daha uzmanlaşmış elemanlar kullanılarak bölünmüştür.
- <History > : Bir el yazması veya el yazması kısmının tam tarihini anlatan grupları elemanları.
- <Additional > : Ek bilgilerin grupları, bir el yazması hakkında bibliyografik bilgileri birleştirerek, ya da küratörlük veya idari bilgilerle bunun vekil kopyaları.
- < msPart > (manuscript part) :Yazmanın bir kısmını oluşturan parça hakkında bilgi içerir.

TEİ'de el yazmalarını tanımlarken aşağıdaki alanlarda da veri girişi yapılması gerekmektedir:

- Boyut ve diğer fiziksel özellikler
- Bir hanedan ya da diğer ilişkiler
- El yazması ya da el yazması parçası içinde konumlar ve yerler
- El yazması ya da el yazması parçası içinde ayrı sayfaların özellikleri
- Kullanılan yazı ve resim özellikleri
- Filigran veya benzeri özellikler
- Kullanılan sözcükler veya nesnelerin özellikleri
- Tarihler ve ilişkili olaylar
- Köken
- İmzalar ve damgalar imzalar

TEI el yazması koleksiyonlarının tanımlanması/kataloglamasına ilişkin yukarıdaki ana başlıklar altında yüzlerce alt başlık ve ayrıntıya yer veren son derece kapmalı standarttır sunmaktadır (TEİ, 2016).

Ülkemizde Yazma Eser Kütüphaneleri Çalışma, Yazma ve Eski Harfli Basma Eserlerden Yararlanma Yönetmeliğine göre el yazmalarının aşağıdaki başlıklarda tanımlanması gerekmektedir (Yazma Eser Kütüphaneleri Çalışma, Yazma ve Eski Harfli Basma Eserlerden Yararlanma Yönetmeliği, 1988).

1- Kitap adı
2- Yazar adı
3- Dil
4- Cilt Adedi ve Numarası
5- Yazıldığı yer/ Basıldığı yer, Tarih ve Basıldığı Matbaa adı
6- Yazının çeşidi ve Yazanın Adı
7- Minyatür, şekil, plan ve harita vb.
8- Tezhip
9- Boyut
10- Yaprak ve Sayfa Sayısı
11- Satır Sayısı

12- Cildin Çeşidi
13- Fiyatı
14- Nereden ve Ne şekilde Geldiği
15- Geldiği Tarih
16- Konu Numarası
17- Eski Kayıt Numarası
18- Düşünceler

Avrupa Birliği Kültüre Mirası ve Arkeolojik Obje Tanımlama Standardı LIDO (Light Information Describing Objects)

LIDO AB projesi olarak başlamış ve ardından kültürel varlıkların ve arkeolojik objelerin tanımlanmasına dönük bir standarda dönüşmüştür. LIDO, kültür kurumları ve müzelerde çevrimiçi koleksiyonların tanımlanmasında yaygın olarak kullanılmaktadır (Sotirova, Peneva, Ivanov, Doneva, & Dobreva, 2012). Organizasyonlar, sahip oldukları nesnelerle ilgili bilgiyi tematik, bölgeler arası, ulusal, uluslararası ve web uygulamaları dahil bir çok yere sağlamak zorundadırlar. Bunun zorluğu; nesnenin bilgisinin, sağlayıcının kendi koleksiyon yönetim sisteminde ve kataloglama veri tabalarında bulunmasıdır. Bunların her biri potansiyel olarak farklı üst veri formatlarına sahiptir. Bu da katılım sağlamak isteyen tüm organizasyonlara zaman kaybı ve maliyet demektir. Bu durumun üstesinden gelebilmek için LIDO geliştirilmiştir. LIDO üçü zorunlu toplam 14 bilgi grubu tanımlar. LIDO kaydında bilgi; 4ü tanımlayıcı 3ü idari karakterde toplam 7 alanda organize edilir.

1) Tanımlayıcı Bilgi

- Nesne Sınıflandırması – Nesnenin türü hakkında temel bilgi
  - Nesnenin Türü (Zorunlu)
  - Nesnenin diğer sınıflandırma terimleri – Örneğin; sitili, formu, yaşı, türü, evresi vs.
- Nesne Tanımlaması – Nesne ile ilgili temel bilgi
  - Başlık (ya da başlık yoksa nesnenin adı)[zorunlu]
  - Kayıt – Deşifre metni(transcript) ve/veya tanımı
  - Depo – Nesneyi fiziksel olarak barındıran organizasyonlar ve kimlikleri
  - Sergi ve yayım bilgisi – Özellikle for prints
  - Betimleme- Betimleyici metin
  - Ölçüler
- Event – Nesnenin yer aldığı olaylar
  - Event ID
  - Event türü
  - Event içinde nesnenin rolü
  - Event adı

- Aktörler (Kişiler ve kurumlar)
- Dahil olan kültürler
- Tarih
- Periyot
- Yerler
- Event metodu
- Kullanınlar materyal ve teknikler
- Event içinde sergilenen diğer nesneler
- Bağlantılı events
- Event'in tanımı

- İlişki – Nesnenin ilişkisi (aşağıda yazanlarla)
  - Konusu (içerik ya da görsel)- Konseptler, aktörler, organizasyonlar, tarihler, yerler ve nesneler
  - Nesneyle direkt olarak bağlantısı olan diğer nesneler

2) İdari Bilgi

- Haklar- Nesneyle ilişkili haklar hakkında bilgi
  - Hakların türü
  - Hak sahibi
  - Hakların tarihi
  - Kredi limiti
- Kayıt - Kayıtla ilgili temel bilgiler
  - Kayıt ID [zorunlu]
  - Kayıt türü [zorunlu]
  - Kaydın kaynağı [zorunlu]
  - Kaydın hakları
  - Sunulan bilgi için üst veri referansları
- Kaynak – Hizmet çevresine sağlanan dijital kaynakla ilgili bilgi
  - Link
  - Kaynak ID
  - İlişki türü – örneğin; muhafaza, tarihi, rekonstrüksiyon
  - Kaynak türü (its medium eg. X-ray)
  - Kaynak hakları
  - Görünüm tanımı
  - Görünüm türü
  - Tarih
  - İlişkili kaynaklar
  - Kaynağın üst veri yeri – Kaynakla ilgili diğer bilgilerin göstericisi (pointer) (Stein, 2012)

Genel Değerlendirme

Standartlaşma daha ilkeli yaşamın temelini oluşturur. Aynı işe dönük farklı uygulamaların benzer süreçleri izleyeceğini bilmek toplumsal güveninin sağlanması için de önemlidir. Standartlaşma iş ve işlemlere dönük süreçlerin katı bir disiplin içerisinde farklılaşan koşullara rağmen hiç değişmeden izleneceği anlamına gelmemelidir. İç ve dış etkenler sürekli izlenerek belirli aralıklarla revize edilen standartlar kurumsal kalite ve verimliliğin sağlanmasına önemli derecede katkı sağlar. Uyumlu ve eşgüdümlü uygulamaların kaçınılmaz olduğu ulusal çaplı organizasyonların ve askeri kuruluşların öncülük ettiği standartlaşma çalışmaları özellikle 2000'li yıllarla birlikte yaygınlaşmış, irili ufaklı hemen hemen tüm organizasyonların bütün iş süreçlerin etkiler hale gelmiştir. Günümüzde devlet vatandaş ilişkilerinden kurum içi ya da kurumlar arası idari ve mali süreçlere, hatta uluslararası ilişkilere kadar ilkeleri belirlenmemiş, yasalara ya da standartlara dayanmayan bir adım atılması mümkün değildir. Bu durum önceden kuralları belirlenmiş karşılaşmalarda mücadelenin ilkelerini belirleyerek süreçlerin sağlıklı yönetilmesi için elzemdir.

Kurumsal belge yönetimi uygulamaları yukarıda bahsi geçen devlet vatandaş ilişkileri, kurum içi ya da kurumlar arası idari ve mali süreçleri, hatta uluslararası ilişkilerin kanıtlanabilir iş süreçlerinin kayıt altına alınmış şeklidir. Bu bağlamda belge yönetimi hiyerarşik ve bürokratik tahakkümlere göre iş ve işlemlerin yazılı ve standart hale dönüştürülmüş şeklidir. Belge yönetiminde standartlaşma özünde belgelerin tabi olduğu koşullara göre şekillenir. Bir başka deyişle iş ve işlemler belirleyen idari koşullar, ilgili süreçlerin kanıtlanabilirliğini ortaya koyan yasal metinler ve bu çerçevede teknolojinin kabul edilen uygulama araçları çerçevesinde belge yönetimi standartları tanımlanabilir. Örneğin elektronik imzanın hangi uygulamalarda hangi kasamda nasıl geçerli olabileceğine dönük düzenlemelerin çerçevesinin dışında bir uygulamanın geçerliliği, her ne kadar bu uygulama çeşitli kanallarca güvenilir bulunsa da tartışmalı hale gelir. Bu bağlamda belge yönetimi standartları özünde kamusal uygulamaların yasal çerçevesinin içerisinde tanımlanmak durumundadır.

Belge yönetiminde ilk standartlar genelde ulusal değil uluslararası düzlemde gelişmiştir. Örneğin Avustralya belge yönetimi standardı olarak ortaya çıkan ilk standart AS 4390 ilerleyen dönemlerde uluslararası belge yönetimi standardı ISO 15489'un temelini oluşturmuştur. 170'in üzerinde üye ülkenin aktif olarak içerisinde yer aldığı uluslararası standartlar örgütü ISO ve ISO'ya bağlı komisyonlarda geliştirilen düzenlemeler hayatın içerisinde er alanı etkiliyor. Doğrudan ya da dolaylı olarak belge yönetimi faaliyetlerine dönük geliştirilen ve çalışma içerisinde ayrıntılarına yer verilen standartlar bu bağlamda belge yönetimi ilkelerini belirliyor. Bu noktada özellikle belge yönetiminde sistem geliştirmek isteyen ancak ilgili konularda güvenilir kaynak bulmakta zorlanan kuruluşlar için ilgili standartlar önemli bir rehber niteliği taşıyor. Çalışmada

standartlar kurumsal bilgi sistemleri ve bilgi merkezlerine dönük uygulamaları belge yönetimi uygulamaları ile birlikte düşünülerek değerlendirilmiştir. Böylece bilgi ve belge yönetimi sistemleri ve uygulamalarına dönük daha geniş ve kapsayıcı bir çalışmanın ortaya çıkarılması amaçlanmıştır. Çalışma içerisinde özellikle elektronik ortamda kurumsal bilgi ve belge yönetimi sistemlerinin geliştirilmesi ve uygulamaların yapılandırılması dönük değerlendirilen uluslararası standartların, ilgili konularda sistem geliştirme sürecinde olan kuruluşlara katkı sağlaması umulmaktadır.

Kaynakça

Archives and Records Assocaition of New Zelland. (2004). *Selected list of national and international standards relating to records and archives*. 09.03.2016 tarihinde http://www.aranz.org.nz/SITE_Default/SITE_resources/standards.asp#2 adresinden erişildi.

ARMA (Association of Records Managers and Administrators). 28 Ocak 2008 tarihinde www.arma.org/erecords/index.cfm adresinden erişildi.

ARMA International. (2006). *ARMA owerview.* 11 Nisan 2016 tarihinde http://www.arma.org/about/overview/index.cfm adresinden erişildi.

ARMA International. (2006). *Standard development, process: setting standards and guidelines for profession*. 18 Nisan 2016 tarihinde http://www.arma.org/standards/development/overview.cfm adresinden erişildi.

Barata, Kımberly. (2004). Archives in the digital age. *Journal of the Society of Archivists, 25 (1):* 63-70

Batley, Sue. (2007). The I in information architecture: the challenge of content management. *Aslib Proceedings: New Information Perspectives*, 59 (2): 139-15.

Bearman, D. (2004). Electronic evidence: Strategies for managing records in contemporary organizations. Pittsburg: Archives and Museum Informatics. 28 Ocak 2008 tarihinde http://www.archimuse.com/publishing/electronic_evidence/ ElectronicEvidence.Intro. adresinden erişildi.

Benedon, W. (1999). Toward the future: the impact issues. *Information Management Journal* 32 (2): 5-6

Bergman, B. K. (1994). *Quality from customer needs to customer satisfaction*. New York: McGraw Hill.

Bilgi Edinme Hakkı Kanunu. (2003). T.C.Resmi Gazete, Sayı: 25269, 24 Ekim 2003: 8617).

Bilgi Güvenliği Teşkilatı ve Görevleri Hakkındaki Kanun Tasarısı. (2007). Türkiye Bilişim Derneği. 30 Mayıs 2007 tarihinde http://www.tbd.org.tr/genel/bizden_detay.php?kod=245&tipi=5&sube= adresinden erişildi.

Blazic, A. J. (2007). Long Term Trusted Archive Services. *Proceedings of the First International Conference on the Digital Society*. 11 Mart 2007 tarihinde http://ieeexplore.ieee.org/iel5/4063752/4063753/04063790.pdf?arnumber=4063790 adresinden erişildi.

Borglund, E. ve Anderson, K. (2010). Checklists for Evaluating the Quality of Recordkeeping. *Proceedings of the 4th European Conference on Information Management and Evaluation: ECIME2010.*

Boudrez, F. (2007). Digital signatures and electronic records. *Archival Science* 7: 179-193

CEN. (2004). Standards and Drafts. European Committee for Standardization, 12 Nisan 2006 tarihinde <http://www.cenorm.be/cenorm/standards_drafts/index.asp adresinden erişildi.

Chain, P. (2002). Model requirement for the management of electronic records (MoReq): A Critical Evaluation. *Records Management Journal* 2002 12(1): 14-18

Charter of the United Nations.(1945). United Nations. 29 Mayıs 2007 tarihinde http://www.un.org/aboutun/charter/ adresinden erişildi.

Cimtech Ltd. (2009). *Managing Information and Documents: The Definitive guide*. 26.03.2012 tarihinde http://www.cimtech.co.uk/Pages/Main/pub_midguide.htm adresinden erişildi.

CDL Guidelines for Digital Objects (CDL GDO). (2011). California Digital Library, University of California. 22 Temmuz 2014 tarihinde http://www.cdlib.org/services/access_publishing/dsc/contribute/docs/GDO.pdf adrsinden erişildi.

Connelly, J. C. (2001) "The new international records management standard: its content and how it can be used". *The Informtion Management Journal* 35 (3): 26-36

Çiçek, N. (2000). ISO 9000 Kalite güvence sistemi standardında evrak üretimi ve yönetimi. *Arşiv Araştırmaları Dergisi*, sayı 2: 7-34

Çiçek, N. (2011). Elektronik belgelerin diplomatik analizi ve arşivsel bağın kurulmasındaki önemi: Türkiye'deki uygulamalar ışığında bir inceleme. *Bilgi Dünyası*, 2011, 12 (1), 87-104.

Darlington, J. F. ve Pearce, P. (2003). Domesday redux: the rescue of the Domesday Project videodiscs. **Ariadne**, (36). 21 Kasım 2007 tarihinde http://www.ariadne.ac.uk/issue36/tna/ adresinden erişildi.

Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik. (2001). T.C.Resmi Gazete, Sayı: 24487, 08 Ağustos 2001: 95-100.

DoD 5015.2: Design Criteria Standard for Electronic Records Management Software Application. (2002). 5 Nisan 2006 tarihinde http://www.dtic.mil/whs/directives/corres/pdf/50152std_061902/p50152s.pdf adresinden erişildi.

Duff, W. and S. McKemmish. (2000). Metadata and ISO compliance. *Information Management Journal* 34(1): 4:15

Duranti, L. (2001). The impact of digital technology on archival science. *Archival Science,* 1 (1):39-55.

Duranti, L, Rogers, C. (2011). Educating for trust. *Archival Science*,11: 373–390.

Elektronik İmza Kanunu. (2004). *Resmi Gazete*, Sayı: 25355, 23 Ocak 2004.

Erturgut, M. (2004). Elektronik İmza Kanunu Bakımından E-belge ve e-imza. Bankacılar Dergisi, sayı 43: 66:79

E-devlet kapısı: devletin kısa yolu. (2014). T.C. Başbakanlık. 28 Ocak 2014 tarihinde https://www.turkiye.gov.tr/portal/dt?provider=HomePageContainer&channel=icerik adresinden erişildi.

E-Güven. (2014). Elektronik Bilgi Güvenliği AŞ. 13 Ocak 2014 tarihinde http://www.e-guven.com/ adresinden erişildi.

E-Tuğra. (2014). Etugra. Retrieved 13 Ocak 2014 tarihinde http://www.e-tugra.com.tr/_eTugra/web/gozlem205a.html?sayfano=1 adresinden erişildi.

Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli. (2006). Hamza Kandur (Hazırlayan). İstanbul: Devlet Arşivleri Genel Müdürlüğü. 1 Haziran 2007 tarihinde http://www.devletarsivleri.gov.tr/EBYS_v_2_0.pdf adresinden erişildi

Enterprise Content Management Association.(2006) AIIM; The Association for Information and Image Management. *About AIIM.* 11 Nisan 2006 tarihinde http://www.aiim.org/article-aiim.asp?ID=18274 adresinden erişildi.

Eroğlu, Ş. (2013). e-Devlet kapsamında kurumsal bilgi sistemlerinin değerlendirilmesi: İçişleri Bakanlığı örneği.European Committee for Standardization. (2004). *CEN: Standards and Drafts*. , 03.02.2006 tarihinde http://www.cenorm.be/cenorm/standards_drafts/index.asp adresinden erişildi.

European Union Interchange of Data Between Administration (IDA) (2008). *Model Requirements For The Management Of Electronic Records (MoReq)*. 16 Mart 2008 tarihinde http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=show.Document&parent=whatsnew&documentID=413 adresinden erişildi.

Evans, D. F. (1998). Cooperation in information management. *Information Management Journal* 32 (4): 32-35

Fanning, B. (2005). Records, e-mail, security standards. *Edocmagazine*. Sept-Oct: 61

Gable, J.(2002). Everything you want to learn about DoD. *Information Management Journal* November/December: 32-38

Glossary of Records Management Terms. (2008). National Arvhives of Australia. 20 Mart 2008 tarihinde http://www.archives.sa.gov.au/management/glossary.html#D adresinden erişildi.

Gringrich, L. (2006). Retention and disposition of structured data: the next frontier for records managers. *The Informaton Management Journal* March-April: 31-39

Haseki, M. T. (2008) Endüstri Standartları ve Patentlerin Üniversite Kütüphanelerine Katma Değeri ve Uygulaması http://www.ulak.net.tr/cabim/ekual/toplanti/izmir/standart_patent.ppt#264,6, adresinden 20.05.2010 tarihinde erişildi.

Herrera-Viedma, E. ve Peis, E. (2003). Evaluating the informative quality of documents in SGML format from judgements by means of fuzzy linguistic techniques based on computing with words. *Information Processing and Management*, 39, 233–249.

ICA. (2009). 12 Şubat 2017tarihinde http://www.ica.org/3/homepage/home.html adresinden erişildi.

Information management planning. (2005). Government of Alberta Information Management Branch. 3 Eylül 2007 tarihinde http://www.im.gov.ab.ca/publications/pdf/IMPlanningGuide.pdf adresinden erişildi.

Information Use Management and Policy Institute. (2006). *Analysis and development of model quality guidelines for electronic records management on state and federal website: website records management in federal agencies.* 7 Nisan 2006 tarihinde http://www.ii.fsu.edu/~cmcclure/nhprc%20/nhprc_chpt_4.html adresinden erişildi

International Organization for Standardization (ISO). (2001). **ISO 15489-1:2001 Information and documentation - Records management - Part 1: General**. Geneva: International Organization for Standardization.

International Council on Archives.(2006). *ICA in brief.* 11 Nisan 2006 tarihinde http://www.ica.org/static.php?ptextid=bref&plangue=eng adresinden erişildi.

International Organization for Standardization (ISO). (2006). *Introduction.* 17 Şubat 2006 tarihinde http://www.iso.org/iso/en/aboutiso/introduction/index.html#thirteen adesinden erişildi.

International Records Management Trust. (2006). About us. 11 Nisan 2006 tarihinde http://www.irmt.org/about.html adresinden erişildi.

InterPARES. (2006). INTERPARES: International Research on Permanent Authentic Records in Electronic Systems: *INTERPARES I-II.* . 7 Nisan 2006 tarihinde http://www.interpares.org/ adresinden erişildi.

InterPARES Authenticity Task Force. (2002). Requirements for assessing and maintaining the authenticity of electronic records. InterPARES, The long-term preservation of authentic electronic records: findings of the InterPARES project. InterPARES, Vancouver. 12 Mart 2008 tarihinde http://www.interpares.org/book/interpares_book_d_part1.pdf. Consulted 2 August 2007 adresinden erişildi.

InterPARES Project. (2008). The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 3 Project. 28 Mary 2008 tarihinde http://www.interpares.org/ adresinden erişildi.

InterPARES 1 Project. (2009). Project summary. 20 Ocak 2012 tarihinde http://www.interpares.org/ip1/ip1_index.cfm adresinden erişildi.

InterPARES 3 Project. (2008). InterPARES 3 Project organizational policy: Final version 2.0. 20 Ocak 2012 tarihinde http://www.interpares.org/display_file.cfm?doc=ip3_organizational_policy_v2-0.pdf adresinden erişildi.

ISO 13008. (2012). Digital records conversion and migration process, 25 Aralık 2016 tarihinde, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52326 sitesinden erişildi.

ISO 13028.(2010). Implementation guidelines for digitization of records, 22 Aralık 2016 tarihinde, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52391 sitesinden erişildi.

ISO 15489. (2016). Records management 15 Aralık 2016 tarihinde, https://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-2:v1:en sitesinden erişildi.

ISO 15489-1. (2001). *International Records Management Standard*. Switzerland: ISO/TC 46 Technical Committee:1-11. 17.02.2006 tarihinde http//www.arxiversvalecians.org/ document/ISO_TR_15489-1pdf. Adresinden erişildi.

ISO 15489-2. (2001) *Technical Report: International Records Management Standard Guidelines*. Switzerland: ISO/TC 46 Technical Committee, 2001:1-24. 17 Şubat.2006 tarihinde http//www.arxiversvalecians.org/document/ISO_TR_15489-2pdf. adresinden erişildi

Kandur, H. (1999). Elektronik arşivler ve arşivcilik mesleğinin geleceği. " Bilgi Çağı, Bilgi Merkezler ve Bilgi Teknolojileri" Sempozyumu bildirileri: 7-8 Mayıs 1997 içinde (ss. 15-21). Ankara: Ankara Üniversitesi.

ISO 23081. (2012). 21 Aralık 2016 tarihinde, http://www.iso.org/iso/home/search.htm?qt=23081&sort=rel&type=simple&published=on sitesinden erişildi.

ISO 30300-30304. (2011). Management systems for records 26 Aralık 2016 tarihinde, http://www.iso.org/iso/home/search.htm?qt=30301&sort=rel&type=simple&published=on sitesinden erişildi.

ISO/TR 26122. (2008). Work process analysis for records, 30 Aralık 2016 tarihinde http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43391 sitesinden erişildi.

İcimsoy, A. O. (1997). Arşivlerde mikroform kullanımı: Yeni teknolojiler ve sorunlar. *Bilgi Çağı, Bilgi Merkezleri ve Bilgi Teknolojileri Sempozyumu 7-9 Mayıs 1997 - Bildiriler* içinde (ss.7-14). Ankara: Ankara Üniversitesi, 1999.

Kampffmeyer, U. (2006). ECM enterprise content management. Project consult: Hamburg. 09 Kasım 2009 tarihinde http://www.project-consult.net/files/ecm_white%20paper_kff_2006.pdf adresinden erişildi.

Kandur, H. (2011). Türkiye'de kamu kurumlarında elektronik belge yönetimi: Mevcut durum analizi ve farkındalığın artırılması çalışmaları. *Bilgi Dünyası*, 12 (1), 2-12.

Kunis, R., Rünger, G. ve Schwind, M. (2007). A model for document management in e-government systems based on hierarchical process folders. *Electronic Journal of e-Government*, 5 (2): 191-204

Külcü Ö. (2006). Küreselleşme sürecince Avrupa Birliği'nde belge yönetimi uygulamaları ve Türkiye. *Bilgi Dünyası* 7 (2): 202-229.

Külcü Ö. (2007). Belge Yönetiminin Değişen Yüzü: Standartlaşma Çalışmaları ve Uluslararası Uygulamalar. Bilgi Dünyası 8 (2): 230-279.

Külcü, Ö. (2009). Evolution of the e-records management practices in e-government: reflections from Turkey. *The Electronic Library,* 27 (6), 999-1009.

Külcü, Ö., Çakmak, T. (2009). Elektronik belge yönetimi üzerine InterPARES Projesi ve Türkiye Takımı faaliyetleri. *Bilgi Dünyası*, 2009, 10 (2), 287-302

Külcü, Ö. (2009). E-Devlet Kapsamında e-Belge Yönetimi Uygulamalarının Gelişimi, Sorunlar ve Beklentiler: Türkiye'den Yansımalar. 8. Ulusal Büro Yönetimi ve Sekreterlik Kongresi (14-15 Ekim 2009). Ankara: Ankara Üniversitesi Hukuk Fakültesi Adalet Meslek Yüksek Okulu.

Külcü, Ö. (2010). Belge yönetiminde yeni fırsatlar: Dijitalleştirme ve içerik yönetimi uygulamaları. *Bilgi Dünyası*, 11 (2), 290-331.

Külcü, Ö. (2012). Türkiye'de Kurumsal Elektronik Bilgi ve Belge Yönetimi Uygulamalarına Dönük Koşulların Değerlendirilmesi: 57 Örnek Kurumun Analizi. Türk Kütüphaneciliği, 26 (1), 7-30

Külcü, Ö. (2013). Ontolojik Çalışmalar Kapsamında Elektronik Arşiv Kaynaklarının Tanımlanması ve Üstveri Alanlarının Geliştirilmesi. Arşiv Emektarlarına Armağan Kitabı içinde (319-352)

Lyman, P. ve Varian, H.R. (2000). How much information. **Journal of Electronic Publishing, 6**(2). 21 Kasım 2007 tarihinde http://www.press.umich.edu/jep/06-02/lyman.html. adresinden erişildi.

MacKenzie, G. (1999). A new world ahead: international challenges for information management. *Informational Managment Journal* 33 (2): 24-34

McFarland, K. (2005). "How to play safe on document retention. *International Financial Law Review*. 24(7): 69-71

McLeod, J., Hare, C. ve Johare, R. (2004). Education and training for records management in the electronic environment - the (re)search for an appropriate model. Information Research 9 (3) 4 Nisan 2008 tarihinde http://informationr.net/ir/9-3/paper179.html adresinden erişildi.

METS Primer Reference Manual. (2007, Eylül). 12 Ocak 2016 tarihinde Library of Congress: http://www.loc.gov/standards/METS adresinden erişildi.

Milli Arşiv Kanun Tasarısı. (2007). Devlet rşivleri Genel Müdürlüğü. 30 Mayıs 2007 tarihinde http://www.basbakanlik.gov.tr/docs/kkgm/kanuntasarilari/milli%20arsiv/milli%20arsiv%20kanunu.doc adresinden erişildi.

Mims, J. (2004). Why records cooperatives. *The Information Management Journal* Nov/Dec. 47-52

Mutula, S. M. ve Brakel, P. (2006). E-readiness of SMEs in the ICT sector in Botswana with respect to information access. *The Electronic Library*, 24 (3): 402-417

National Archives of Australia. (2006). Archiving web sources. 5 Nisan 2006 tarihinde http://www.naa.gov.au/recordkeeping/er/web_records/intro.html adresinden erişildi.

National Archives of United Kingdom. (2002). Functional requirements for electronic records management systems. 5 Nisan 2006 tarihinde http://www.nationalarchives.gov.uk/electronicrecords/function.htm adresinden erişildi.

National Research Institute of Electronics and Cryptology. (2008). 28 Mart 2008 tarihinde http://www.uekae.tubitak.gov.tr/home.do?ot=10&lang=en adresinden erişildi.

Niu, J. (2013). Recordkeeping metadata and archival description: a revisit. *Archives and Manuscripts, 41*(3), 203-215.

Odabaş, H. (2007). *Elektronik belge yönetimi ve kamu kurum ve kuruluşları.* Yayımlanmamış doktora tezi, Ankara: Ankara Üniversitesi.

Organization for Economic Co-opretation and Development (OECD).(2007). About OECD. 29 Mayıs 2007 tarihinde

http://www.oecd.org/about/0,2337,en_2649_201185_1_1_1_1_1,00.html adresinden erişildi.

Özdemirci, F. (1996). *Kurum ve kuruluşlarda belge üretiminin denetimi ve belge yönetimi.* İstanbul: Türk Kütüphaneciler Derneği İstanbul Şubesi Yayınları.

Özdemirci, F. (2003). İlk uluslararası belge yönetim standardı: ülkemiz açısından bir değerlendirme. *Türk Kütüphaneciliği*, 17: 3: 225-246.

Özdemirci, F. (2008). Government records and records management: Law on the right to information in Turkey. *Government Information Quarterly*, 25 (2), 303-312.

Pember, M. (2006). Sorting out the standards: What every records and information Professional should know. *Records Management Journal*, 16(1), 21-31.

Pemperton, J. M. (1997). Canadian information professionals sound the ALARM and ARMA and SAA reach out. *Records Management Quarterly* October 1997, 31: 62-64

PRISM International. (2006). *About PRISM International*. 11 Nisan 2006 tarihinde http://www.prismintl.org/about.php adresinden erişildi.

Reed, B. (2005). Records. *Archives:recordkeeping in society,* McKemmish, S, Piggott, M., Reed, B. and Upward, F.(Eds.). Wagg NSW, Centre for Information Studies,

Resmi yazışmalarda uygulanacak esas ve usuller hakkında yönetmelik. (2015). *T. C. Resmi Gazete*, Sayı: 29255.

Rosenfeld, L. and Morville, P. (2002). Information Architechture for World Wide Web. Sebastopol: O'Reilly & Associates.

Schlickman, J. (2003). *ISO 9001:2000 Quality management system design*. Boston: Artech House

Shepherth, E. and R. Pringle. (2002). Mapping descriptive standards across domains: a comparision of ISAD (G) and SPECTRUM*". Journal of the Society of Archivists* 23 (1): 17-34

Shepherd, E. and V. West. (2003). Are ISO 15489-1 2001 and ISAD(G) compatible? Part 1". *Records Management Journal* 13 (1): 9-23

Spratt, R. (2004). Records management: the next ten years. RDIMS (Records, Documents and Image Management Systems). Canadian Federal Government Shared System Initiative . Retrieved March 17, 2008, from http://www.rdims.com/Documents/WhitePaper-Records Management-The NextTenYears.doc.

Sprehe, T. J. (2005). Integrating records management into information resources management in US government agencies. *Government Information Quarterly* 17 (1):13-26

Standart Dosya Planı. (2005). T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü

Genelge, Sayı: 320–3802, 24 Mart 2005.

Stein, R. (2012, Mayıs 23). *Europeana, Standards and Aggregation of Content: The LIDO Model*. Stockholm.

Stephens, D. O. (2001). Megatrends in international records management. *Information Management Journal* 35 (4): 66-70

Stephens, D. O. (2005). The why and how of international records retention. *Information Management Journal*. Sept-Oct: 29-35

Sundberg, H.P. and Wallin, P. (2007). Recordkeeping and information architecture. *International Journal of Public Information Systems*,1: 31-45

Şahin, E. (2016). Elektronik Belge Yönetimi Sistemlerinde ISO Standartları. Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü. Yayımlanmamış Rapor.

T.C. Başbakanlık Dış Ticaret Müsteşarlığı(2007). Dünya Ticaret Örgütü ve Türkiye. 29 Mayıs 2007 tarihinde http://www.dtm.gov.tr/dtmweb/index.cfm?action=detay&yayinID=285&icerikID=385&dil=TR adresinden erişildi.

TEİ, (2016). 12 mart 2017 tarihinde http://www.tei-c.org/release/doc/tei-p5-doc/en/html/MS.html adresinden erişildi.

The Society of American Archivists. (1999). Standards for archival description: a handbook. Compiled by Victoria Irons Walch. 7 Nisan 2006 tarihinde

Thurston, A. (2005). Fostering trust and transparency through information systems. *ACARM Newsletter*, *36*, 1-5.

Türk Standartları Enstitüsü Standart Hazırlama Merkezi.(2007). Standart Tasarısı: ISO 15589-1. (2007). 10 Mayıs 2007 tarihinde https://www.tse.org.tr/turkish/abone/Standard Detay.asp?STDNO=45399&sira=0 adresinden erişildi

TS 13298. (2015). *Elektronik belge yönetimi*. Bilgi Teknolojileri ve İletişim İhtisas Grubu Türk Standartları Enstitüsü. 13 mart 2017 tarihinde https://www.tse.org.tr/tr/icerikdetay/946/1217/ts-13298-ebys-genel-bilgiler.aspx adresinden erişildi.

TS EN ISO 9001: 2000. (2001). *Kalite Yönetim Sistemleri: Şartları*. TSE:Ankara, 1-22 http://www.archivists.org/catalog/stds99/ adresinden erişildi.

TS EN ISO 9001. (2008). *Kalite yönetim sistemleri: şartları*. TSE: Ankara.

TS ISO 15489-1. (2007). *Bilgi ve dokümantasyon- Belge yönetimi Bölüm 1: Genel*. Ankara: Türk Standardları Enstitüsü.

TS ISO/TR 15489-2. (2007). *Bilgi ve dokümantasyon- Belge yönetimi Bölüm 2*: *Genel*. Ankara: Türk Standardları Enstitüsü.

ISO 15489-1:2016. (2016). Information and documentation -- Records management -- Part 1: Concepts and principles. 21 Mart 2017 https://www.iso.org/standard/62542.html adresinden erişildi.

Turktrust. (2014). Turkstrust. 13 Ocak 2014 tarihinde http://www.turktrust.com.tr/ adresinden erişildi.

Türk Standartları Enstitüsü. (2007a). Bilgi ve dokümantasyon – Belge yönetimi (TSE ISO 15589-1. (2007). 1 Kasım 2007 tarihinde https://www.tse.org.tr/turkish/abone/StandardDetay.asp?STDNO=45399&sira=0 adresinden erişildi.

Türk Standartları Enstitüsü. (2007b). Bilgi ve dokümantasyon –Elektronik belge yönetimi. (TSE 13298). 1 Kasım 2007 tarihinde http://www.tse.org.tr/Turkish/Abone/Standard_Ara.asp?Durum=IcsTablosu&Sira=1&EskiKod=01.110 adresinden erişildi.

United Nations. (1996). *Model law on electronic commerce*. Retrieved 13 Nisan 2007 tarihinde http://www.unescap.org/tid/projects/ecom04_s4sorieul.pdf adresinden erişildi.

United Nations. (1998). *E-commerce legal issues*. Retrieved 13 Nisan 2007 tarihinde http://www.unescap.org/tid/gateway/tisgway_ecom.pdf adresinden erişildi.

Upward, F. (2000). Modeling the continuum as paradigm shift in record keeping and archiving processes, and beyond – a personal reflection. Records Management Journal, 10 (3): 115-139.

Waldron, M. (2004). Adopting electronic records management: European srategic initiatives. *The Information Management Journal*. July/August 2004:31-35

Wamukoya, J. ve Mutula, S. M. (2005). For e-records management the case in East And Southern Africa. *Records Management Journal,* (15) 2: 71-79

Yazma Eser Kütüphaneleri Çalışma, Yazma ve Eski Harfli Basma Eserlerden Yararlanma Yönetmeliği. (1988). Kültür ve Turizm Bakanlığı. 12 Mart 2017 tarihinde http://www.resmigazete.gov.tr/eskiler/2003/04/20030409.htm#6 adresinden erişildi.

Standartlar Çerçevesinde EBYS ve e-Arşiv Uygulamalarında Kurumsal Yeterlilik Gereksinimini ve Nitelikli İnsan Gücünü Geliştirme Faaliyetleri

Uzm. Zeynep AKDOĞAN

Ankara Üniversitesi BEYAS Koordinatörlüğü; Ankara Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı Doktora Öğrencisi

Prof. Dr. Fahrettin ÖZDEMİRCİ

Ankara Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Öz

Elektronik belge yönetim sistemleri (EBYS) ve e-Arşiv uygulamaları, ilgili ulusal/uluslararası norm ve standartlar ile ilgili kurumsal gereksinimler çerçevesinde oluşturulmaktadır. Bilgi ve iletişim teknolojilerindeki hızlı gelişmelerin uygulamalara doğru ve eksiksiz biçimde yansıtılması uygulamaların işlevselliği bakımından önem taşımaktadır. Dinamik yapıya sahip uygulamaların genel olarak bilgi ve belge yönetimi ile bilişim-teknoloji altyapı boyutu bulunmaktadır. EBYS ve e-arşiv uygulamalarında çalışacak personelin belge yönetimi, bilişim sistemleri, bilgi güvenliği, bilgi sistemleri entegrasyonu ve diğer konularda bilgi sahibi olmaları gerekmektedir. EBYS ve e-arşiv uygulamalarına yönelik yapılacak eğitimler, uygulamaların hizmet kalitesini arttıracaktır. Bununla birlikte kurumlarda yetişmiş insan gücü, uygulamaların daha iyi yönetilmesine ve geliştirilmesine katkı sağlayacaktır. Bildiride, EBYS ve e-arşiv uygulamalarında yetişmiş insan gücü gereksinimi, AÜ ve TSE'nin yapacağı eğitimler kapsamında irdelenecektir.

Anahtar Kelimeler: *TS 13298, EBYS, e-Arşiv, Eğitim*

Giriş

Ülkemizde pek çok kurum elektronik belge yönetim sistemlerini (EBYS) kullanmaktadır. Kurumlarda kullanılan EBYS uygulamalarının belge yönetimi ve arşiv disiplini, ulusal ve uluslararası standartlar, hukuk kuralları çerçevesinde doğru ve etkin kullanılması için pek çok başarı kriteri bulunmaktadır. Başarı kriterlerinin ilk sıralarında kurumsallaştırma, belge yönetimi ve arşiv sisteminin kurumda tamamlanmış olması, üst yönetim desteği, personel eğitimi ile ilgili konu

uzmanlarının EBYS uygulamasının her sürecine (oluşum, gelişim, yönetim) dâhil edilmesi yer almaktadır (Akdoğan ve Özdemirci, 2016, s.54). Kurumlarda EBYS uygulamalarında yer alan her düzeyde kullanıcının (personelin) sürekli eğitimine ihtiyaç duyulmaktadır.

Kurumlarda EBYS ve e-Arşiv sistemlerinde çok farklı alanlardan insan gücüne ihtiyaç bulunmaktadır. *Üst yöneticiler*, kurumlarda EBYS ve e-Arşiv sistemlerini destekleyerek ve sürdürülebilirliğini sağlayan kişilerdir. *Bilişimciler,* EBYS ve e-arşiv sistemlerinin teknik altyapısını oluşturan, diğer bilgi sistemleri ile teknik entegrasyonu gerçekleştiren, teknolojik olarak sistemin sürdürülebilir ve güncel yapısını koruyan kişilerdir. *Belge yöneticisi ve arşivciler,* kurumun belge yönetimi ve arşiv yapısını oluşturan, EBYS ve e-Arşiv sisteminin iş akışlarını belirleyerek arşivcilik yöntem ve tekniklerine göre sistem mimarisini bilişimcilerle beraber oluşturan kişilerdir. *Kurumun tüm çalışanları ise* EBYS ve e-Arşiv uygulamaları süresinde yer alan kişilerdir. Bir kurumda kapsama alanı bu kadar yaygın olan, iş süreçlerinin yürütüldüğü e-Belge yönetimi ve e-Arşiv sistemlerinin etkin ve sürdürülebilir biçimde oluşturulması ve kullanılması her düzeyde eğitimleri gerektirmektedir. Bu bağlamda e-Belge yönetimi ve e-Arşiv uygulamaları, belge yöneticisi ve arşivciler ile bilişimcilerin EBYS ve e-Arşiv sistemlerine ilişkin eğitimleri birlikte yürütmelerini ön plana çıkarmaktadır. Kurumlarda EBYS ve e-Arşiv sistemlerine yönelik verilecek eğitimlerin personelin görev ve sorumluluklarına göre kademeli olarak verilmesi önemli noktalardan birisini oluşturmaktadır. EBYS ve e-arşiv sisteminde personelin yapacağı işlemleri içeren teorik ve uygulamalı eğitimler birlikte yürütülmelidir. Belge yönetimi ve arşiv disiplini literatürüne önemli katkılar sağlayan Cook arşiv otomasyon sistemlerine yönelik verilecek eğitimlerin, teoriler ve genel prensipler çerçevesinde verilerek personelin sistemin çalışma mantığını doğru şekilde kavraması açısından yararlı olacağını vurgulamaktadır (Cook, 1992, s.10). Eğitimler, kurumlarda EBYS ve e-Arşiv sisteminin önemi, boyutları, iş süreçlerine etkileri ve personelin iş süreçlerinde sistemi en iyi nasıl kullanacağı gibi noktalara odaklanmalıdır.

EBYS ve e-Arşiv Sistemlerinde İnsan Gücü Gereksinimi

e-Belge yönetimi ve e-Arşiv sistemlerinin bir kurumda etkin olması: iki temel unsura bağlıdır. **Birincisi**, etkin kurumsal yapılar; **ikincisi**, yetki ve sorumluluklardır. Bu unsurlar net olarak ortaya konulmadan e-Belge yönetimi ve e-Arşiv sistemleri bir kurumda etkin olarak yönetilememekte; en iyi, en nitelikli olarak tanımlanan yazılımlara sahip olmak yetmemektedir. Teknolojinin geldiği noktada meseleye yalnızca bir bilişim ve mühendislik alanı üzerinden bakmamak gerekmektedir. Bilişim alanından belki daha da etkili ve insanlık tarihini

yönlendirecek olgu, bilgiyi yenilikçi bilgi sistemlerini kullanarak yönetebilmektir.

Bu bağlamda, e-Belge yönetimi ve e-Arşiv sistemlerinde ihtiyaç duyulan ürünlerin ve yazılımların standartlara uygunluğunun sertifikalandırılması yetmemekte; kurumların bilgi sistemi süreçlerini yönetebilme yeteneği, iş ve işlem süreçlerini e-ortamda yürütme becerisi ve başarısı, e-Belge yönetimi ve e-Arşiv sistemlerini kullanma yetkiliğinin ölçülmesi ve sertifikalandırılması gerekmektedir. Kurum ve kuruluşlar olarak bizler bu konuda ne kadar hazırlıklıyız, bilgi varlıklarımızı ve bilgilerimizi bilgi sistemlerinde ne kadar düzgün yönetebileceğiz, bunun için teknoloji tek başına yeterli olacak mı? Bu açıklamalar ışığında şu tespitte bulunabiliriz, e-Belge yönetimi ve e-Arşiv çalışmaları disiplinler arası çalışmaları gerektirmektedir. Bu alanın gerektirdiği farklı formasyona sahip kişilerin birlikte çalışabilmesi için, ortak bir platformda buluşabilmesi için, e-Belge yönetimi ve e-Arşiv alanında eğitimlere ihtiyaç olduğu açıktır.

Belge yöneticisi ve arşivciler sadece belge-bilginin toplanmasında, depolanmasında değil, değerlendirilip analiz edilmesinde ve yeni teknolojilerin kullanımında etkin olmalıdır. "Belge merkezleri ve arşivler, geleceğin 'Veri Merkezleri'dir. Artık 'Kurum Arşivi' olmayacak, 'Kurum Veri Merkezi' olacak, bu veri merkezlerinde biz belgeyi nasıl yönetiriz. Sanırım üzerinde durulması gereken önemli hususlardan birisi de budur. Yeni ufuklar, yeni kuramsal yaklaşımlar gerektirir" (Özdemirci, 2017, 229.s.). Belge yöneticileri ile bilişimcilerin birlikte çalışması, alanı ileri götürmek için şarttır. Belgenin/bilginin e-ortamda etkin, güvenilir üretimi ve yönetimi, işbirliklerinin yapılmasını, deneyimlerin paylaşılmasını gerektirmektedir. Ülkemizde çok değerli yazılımcılar var, ancak kurguya da ihtiyaç var, sistematize etmeye de ihtiyaç var. Biz bunları yapabilirsek, ihtiyaçlarımızı ortaya koyabilirsek, **yerli yazılımların niteliği de artacaktır**.

Kurumlar bundan 10, 20, 50, 100 yıl sonra kendilerini nerede görmek istiyorlar? Yol haritalarını ona göre çizecekler, e-Belge yönetimi ve e-Arşiv sistemlerini ona göre şekillendirecekler. e-Belge yönetimi ve e-Arşiv sistemlerinin etkin ve sürdürülebilir platformlarda yönetimi kurumlarımızın, toplumumuzun, devletimizin geleceğidir. Artık elektronik belge yönetimi ve elektronik arşivler bilgi sistemlerinin ve bilişim yönetiminin en önemli ve en büyük alanını oluşturmaya başlamış, bilgi sistemlerin baş aktörü haline gelmiştir. Elektronik belge yönetimi ve e-arşiv uygulamaları, e-imzanın kullanımını hızla yaygınlaştırmış, güvenli belge-bilgi üretmenin ve paylaşmanın en güzel örneklerini oluşturmuştur. Kapsama alanı, etkileri çok geniş ve çok çok uzun soluklu olan başta e-Belge yönetimi ve e-Arşiv sistemleri olmak üzere bilgi sistemleri ve bilişim yönetimi uygulamalarının geliştirilmesinde, yönetilmesinde

ve kullanımında bilgi/belge yöneticileri ve arşivciler, bilişimciler, bilgisayar mühendisleri, yazılım mühendisleri, yönetim bilimciler birlikte çalışmalıdır.

Disiplinlerarası yaklaşımla yapılmasının gerekli olduğu öngörülen eğitimlerin, e-Belge yönetimi ve e-Arşiv sistemlerinin gerek geliştirilmesinde gerekse etkin olarak uygulanmasında birlikte çalışılması gereken uzmanların beraber çalışmalarını sağlamaktır. Bu sağlandığında ise e-Belge yönetimi ve e-Arşiv sistemleri kurumlarda etkin, güvenli ve sürdürülebilir bir yapıya kavuşturulabilecektir.

Ankara Üniversitesi ve Türk Standartları Enstitüsü: TS 13298 Eğitimleri

Ülkemizde EBYS ve e-arşiv uygulamalarında, TS 13298 Elektronik Belge ve Arşiv Yönetim Standardı, alana yönelik diğer düzenlemeler ve mevzuat hakkında bilgi, beceri ve yetkinliğe sahip nitelikli insan gücüne ihtiyaç bulunmaktadır. Bu ihtiyacı gidermek amacıyla Ankara Üniversitesi (AÜ) ile Türk Standartları Enstitüsü (TSE) arasında 11.04.2016 tarihinde işbirliği protokolü imzalanmıştır. İmzalanan protokol standardizasyon, uygunluk değerlendirme, belgelendirme, elektronik belge, e-arşiv bilgi yönetimi ve bilişim sistemleri alanlarında ortak çalışmalar yapmasına yönelik işbirliği yapılmasına yöneliktir. Protokol kapsamında, kamuda TS 13298 Standardı çerçevesinde EBYS ve e-arşiv uygulamalarına yönelik eğitimler, karşılaşılan sorunlar ve çözüm önerileri, standartlaşma ile EBYS alanında nitelikli personel yetiştirilmesi hususlarında çalışmalar yapılmaktadır.

TS 13298 Elektronik Belge ve Arşiv Yönetim Sistemi Standardı (2015 revizyonu ile) Ürün Sertifikasyonu ve Kurum Yeterlilik Sertifikasyonu olmak üzere iki sertifikalama getirmektedir. Kurum Yeterlilik Sertifikasyonu kurum EBYS süreçlerini yönetebilme yeteneği, iş ve işlemlerin EBYS ortamında yürütme becerisi ve başarısı, mevzuata uygun iş ve işlem süreçlerinin yürütülmesi gibi yetkinliklerinin ölçülmesi hedeflenmektedir (TS 13298, 2015).

Kamu kurumlarının 31.07.2017 tarihine kadar, Üniversite ve Belediyelerin ise 31.12.2017 tarihine kadar EBYS'ye geçmesi için Başbakanlık Müsteşarlığının Mayıs 2017'de aldığı karar göz önüne bulundurulduğunda, EBYS uygulamalarının tüm kamu kurum ve kuruluşlarını kapsayacağı açıktır. 2017/21 sayılı e-Yazışma Projesi konulu Başbakanlık Genelgesi'nde 158 kamu kurum ve kuruluşunun EBYS kullanmaya başladığı belirtilmektedir (e-Yazışma Projesi, Genelge, 2017) Kamu kurum ve kuruluşlarının EBYS kullanmaya yönlendirilmeleri, e-Arşivlerin de hızla kurumların gündemine girmesine neden olmaktadır. Kurumlarda bilgi ve belge yönetimi disiplininin öngördüğü yöntem ve tekniklere uygun sürdürülebilir EBY ve e-Arşiv uygulamaları ise bilişim

personeli, bilgi ve belge yöneticilerinin sistem içinde aktif olarak görev almalarını gerektirmektedir.

Bu bağlamda Türk Standartları Enstitüsü (TSE) ve Ankara Üniversitesi arasında 11 Nisan 2016 tarihinde imzalanan standardizasyon, uygunluk değerlendirme, elektronik belge ve arşiv yönetim sistemi ile bilişim sistemleri alanlarında işbirliği gerçekleştirilmesini içeren protokol çerçevesinde Ankara Üniversitesi Bilgi Yönetim Sistemleri Belgelendirme Merkezi (BİL-BEM), Ankara Üniversitesi Uzaktan Eğitim Merkezi (ANKUZEM), Türk Standartları Enstitüsü (TSE) birlikte çalışmalarını sürdürmektedir.

Kurum ve kuruluşların bu yetkinlikleri kazanabilmesi için bu alanda ilgili bilgi birikimi olan insan gücüne olan ihtiyacı karşılamayı bir kamusal sorumluluk olarak gören Ankara Üniversitesi ve TSE birlikte Uzaktan Eğitim Teknolojileri ve Yöntemleri kullanılarak Sertifika eğitimi çalışmaları başlatmıştır.

Eğitimin Genel Kapsamı şu şekildedir;

- Elektronik Belge ve Arşiv Yönetim Sistemi ile ilgili mevzuat ve standartlar, TS 13298
- Elektronik Belge ve Arşiv Yönetim Sistemi Standardı çerçevesinde Kurum Dosya Planı, Saklama Planı, EBYS Kullanım Özellikleri
- Kurumlarda EBYS’ye Geçiş ve EBYS Yönetimi
- EBYS İç ve Dış Entegrasyonlar
- Teknik Altyapı- Denetim- Güvenlik- Süreklilik ve Sürdürülebilirlik
- Bilgi Güvenliği
- Standardizasyonun Önemi ve Süreçleri

Ana hatlarıyla bu kapsamda planlanan eğitim programının amacı:

- Kamu kuruluşları ve özel sektörde, başta TS 13298:2015 Standardı olmak üzere ilgili mevzuata uygun olarak elektronik belge ve arşiv yönetim işlemlerini yürütebilmeyi sağlayacak yaklaşım, yol, yöntem ve teknikleri öğretmek ve uygulama becerisi kazandırmak.
- Kurum ve kuruluşlarda elektronik belge ve arşiv yönetim süreçlerinde çalışan, çalışmak isteyen kişilerin bilgi, beceri ve yetkinliklerini arttırmak.
- Kurumların idari etkinlikleri sonucu elektronik belge yönetim sistemlerinde oluşan güncel ve geriye dönük belge birikimi ve bilgi akışının iş/hizmet odaklı, kurumun örgütsel ve idari yapısı uyarınca önceden belirlenmiş elektronik belge yönetimi politikasına göre sistematik kurallar doğrultusunda yönetilip işletilmesi becerilerini arttırmak.
- Elektronik belge ve arşiv yönetim uygulamalarını etkin yürütmesini sağlayacak beceri ve kazanımlara sahip insan gücü alt yapısını geliştirmek olarak özetleyebiliriz.

Sonuç

Kamu ve özel sektörde kurumsal, yönetimsel dinamikler ve teknolojik gelişmelere bağlı olarak elektronik belge ve arşiv yönetim sistemleri her geçen gün kurum ve kuruluşlarda hayata geçirilmekte ve hatta zorunlu tutulmaktadır. Elektronik belge ve arşiv yönetim sistemi uygulamaları kurum ve kuruluşlarda nitelikli personelin varlığını her geçen gün daha da artırmaktadır.

EBYS Uygulamalarına geçen kurumların, EBYS uygulamalarına yönelik politikalarını, stratejilerini, prosedürlerini ve eylem planlarını doğru ve eksiksiz biçimde geliştirmeleri kurumlarında ilgili konuda yetişmiş insan gücüne bağlıdır. Personel eğitimi ile kurumlarda EBYS uygulamalarına yönelik ***farkındalık*** ve ***bilinç*** oluşturulacaktır. Değişim ve dönüşüm iyi yönetilemez ise kurumlar belleklerini kaybetmek ile karşı karşıya kalacaktır. Kurumlar güvenli ve sürdürülebilir EBYS ve e-Arşiv sistemlerini hayata geçirerek kurumsal belleklerini geleceğe taşıyabileceklerini göz ardı etmemelidir.

Kaynakça

Akdoğan, Z., Özdemirci, F. "e Process of Institutionalization of Electronic Records Management Systems in Universities: Ankara University e-BEYAS Application", Journal of Communication and Computer, 13 (2016) 50-54. doi:10.17265/1548-7709/2016.01.008.

Cook, Michael, Arşiv otomasyonuna giriş: bir ramp çalışması. Ankara: Başbakanlık Devlet Arşivleri Genel Müdürlüğü Cumhuriyet Arşiv Dairesi Başkanlığı, 1992.

e-Yazışma Projesi, Genelge (2017/21). T.C. Resmi Gazete, (30210), 14 Ekim 2017.

Özdemirci, F. "Belge ve Arşiv Yönetiminde Yeni Ufuklar ve Kuramsal Yaklaşımlar". **Bilgi ve Belge Yönetimi: Kuramsal Yaklaşımlar**/ Yayına hazırlayanlar: Bülent Yılmaz, Turgay Baş, Semanur Öztemiz, Meltem Dişli.- İstanbul: Hiperlink, 2017. İçinde 219-232. ss.

TS 13298 Elektronik Belge Ve Arşiv Yönetim Sistemi. Ankara: TSE, 2015.

E-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme

Influence of the Archival Bond of E-Records to the Digital Forensics: A Survey in the Context of Records Management Literature

Prof. Dr. Niyazi ÇİÇEK
İstanbul Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Özhan SAĞLIK
İstanbul Üniversitesi

Öz

Örgütlerde fonksiyonların yürütülmesi sırasında işlemlerin delili olan e-imzalı belgelerin uzun süreli saklanmaları durumunda, özgünlüğünü muhafaza edemeyeceği tartışmaları gündemi meşgul etmektedir. Zaman içerisinde e-imzanın geçerliliğini yitireceği, belge ile üstverilerin bütünlüğünün sağlanamayacağı, belgenin türüne göre karakteristik özelliklerini koruyamayacağı, ait olduğu dosya ve diğer belgelerle ilişkisinin kopacağı kaygıları, bu tartışmaların başlıca sebebi olarak görülmektedir. E-belgelerde doğabilecek bu özgünlük probleminin onun delil değerini kaybettirme ihtimali yüksektir. Daha çok dijital ortamın kırılganlığı ve yazılımsal sorunlar nedeniyle ortaya çıkacağı düşünülen bu olumsuzlukların, arşivsel bağın tam olarak kurulamamasından kaynaklanabileceği akla gelmektedir. Belgelerin form özelliklerini kullanarak üreticisi ile aynı fonksiyon kapsamındaki diğer belgeler ve ait olduğu dosyayla ilişkisini tespit etmeye imkân veren arşivsel bağ, belge hiyerarşisini açığa çıkarmayı sağlar. Bu bağın tesis edilememesi durumunda, belgenin delil değerinin olumsuz yönde etkileneceği düşünülmektedir. Bu çalışmada "elektronik delil elde etme yöntemi olarak arşivsel bağın kullanılabileceği" hipotezi savunulmaktadır. Çalışmada betimsel analiz yönteminden faydalanılmıştır. İçerikten dolayı mevzunun bilişim, idare hukuku, hukuk muhakemeleri usulü alanlarıyla ilişkisi bulunmaktadır. Burada konu, daha çok belge yönetimi ve arşivcilik literatürü ışığında incelenecektir. Türkçe ve yabancı dil kaynaklarda e-belgelerin arşivsel bağının kurulmasını irdeleyen çalışmalar bulunsa da bu bağın belgenin delil değeri ile olan ilişkisine yeteri kadar girilmemiştir. Bu makalede, belge yönetimi uygulamalarında müstakil bir üstveri alanı olarak kurgulanması gerektiği vurgulanan arşivsel bağın, elektronik delil elde etme yöntemi olarak da değerlendirilebileceği savunulmaktadır.

***Anahtar sözcükler**: E-Belge, E-Arşiv, Arşivsel Bağ, Elektronik Delil Elde Etme Yöntemleri*

Abstract

In case of preserving e-signatured records in long term which are the evidence of processes while carrying out the functions in organizations, debate of not maintaining authenticity is occupying the agenda. Expiring validity of e-signature over time, not ensuring integrity of the records and its metadata, not protecting its characteristic features upon the genre of a record, anxiety of breaking off the relationship with its belonging file and other records have been seen the main reasons of this debate. Probability about losing its evidential value of this authenticity problem that could be rise on e-records is high. These negativeness thought to be occurred from fragility of digital environment and software reasons derived from not determining the archival bond have came to mind. Archival bond is ensuring to expose record hierarchy by using the form features of records that enables to determination of relationship between the creator of a record and other records that have more or less the same function and its belonging file. In case of not establishing this bond, it has been thought the evidential value of records affected negatively. "Adopting archival bond as a digital forensics method" has been argued as a hypothesis in this study. Descriptive analysis method has been benefited in the research. Because of the content, subject is related with forensics, administrative law and civil procedure. In here, subject has been examined in the light of records management and recordkeeping literature. Even there are researches scrutinizing the determination of e-records' archival bond in Turkish and foreign language resources, relationship of this bond with the record' evidential value has not been enough evaluated. In this article, besides emphasizing the need of adopting as a separate metadata field in the records management applications of archival bond, it could be evaluated as a digital forensics method has been asserted.

Keywords: *E-Record, E-Archive, Archival Bond, Digital Forensics*

Giriş

Kamu kurumlarında oluşan belgelerin muhafaza edilmesinin önemli bir sebebi, idari işlemlerin delili olmalarından dolayıdır. Belgeler bu delil değeriyle, yapılan faaliyetlere ispatlık eder. Bunun için yazılı bir kaydın belge olabilmesi için bir takım hukuki niteliklere sahip olması gerekir (Çiçek, 2009, s.109). Aynı özellikler, belgenin delil vasfını koruyabilmesi için de geçerlidir.

Her ne kadar bu nitelikler genel kabul görse de teknolojik ve hukuki gelişmeler ışında bir takım farklı enstrümanlar olduğu ve bunlara bağlı olarak yeni yaklaşımlar bulunduğu bilinmektedir. Belgelerin hangi özelliklere sahip olduğu takdirde delil değerini muhafaza edeceği çeşitli kanunlarda ve Yargıtay kararlarında da ifade edilmiştir. Söz konusu özellikler şöyle açıklanabilir: İrade beyanı içermek, somutluk ve yazılılık (Berkin, 1946; Acar, 2012, s. 142-144); anlaşılıp, kabul edilebilirlik (Henkoğlu, 2014, s. 6); gerçeklik ve ispatı sağlamaya yönelik ilişkiyi gösterebilmek (Ceza Muhakemesi Kanunu, 2004; Yargıtay, 2013; Değirmenci, 2014, s. 114-115; Özen ve Özocak, 2015, s. 57). Bunlara ek olarak delil toplama sürecinde delillerin gerçekliği ve güvenilirliğine gölge düşürmemek, inandırıcılık ve mahkemenin takdirine sunulabilirlik (Yargıtay,

2013; Değirmenci, 2014, s. 114-115; Henkoğlu, 2014, s. 7), aynı zamanda muhakeme taraflarınca delillerin bilinmesinin sağlanması (müştereklik) ile delilin oluştuğu andan imhasına kadar geçen süreçte doğruluğunun ve bütünlüğünün sağlanması olarak değerlendirilmektedir (Yargıtay, 1993; Değirmenci, 2014, s.114-115; Özen ve Özocak, 2015, s. 58).

Genellikle taşıyıcı ortamı kâğıt olan belgeler için öngörülen bu kriterlere, elektronik belgeler göz önüne bulundurulduğunda yeni yaklaşımların olması gerektiği görülmektedir. Bir belgenin yukarıda belirtilen delil olma hususiyetlerini dikkate alarak e-belgelerin sahip olması gereken özellikleri araştıran belge yönetimi uzmanları, belgelerin bütünlük ve özgünlükleri ile e-imzanın varlığı gibi karakteristiklerini ön plana çıkarmıştır (The International Research on Permanent Authentic Records in Electronic Systems [INTERPARES], 2008a; Digital Record Forensics, 2011). Belgelerin bu özellikleri korunduğu zaman delil değerinin muhafaza edilebileceği düşünülmektedir. Ayrıca, delilin oluştuğu andan imhasına kadar geçen süreçte doğruluğunun ve bütünlüğünün sağlanması gerekmektedir. Bu durumda, delil değerinin muhafazasında belgelerin bütünlük ve öz niteliklerinin korunması ile e-imza doğrulamasının önemli bir konumda olduğu görülmektedir. Delil değerinin muhafazasında daha çok e-imza doğrulama yöntemlerinden yararlanılır. E-imzanın belgedeki irade beyanına yönelik kimlik tespiti işlevi nedeniyle bu yaklaşım tabii görülebilir. Fakat, belgelerin uzun süreli saklanmaları durumunda özgünlüğünü muhafaza edemeyeceği tartışmalarının gündemi meşgul ettiği bilinmektedir (Archive of New Zealand, 2017; Stancic, 2016; Denham, 2017). Bu tartışmaları, belgelerin delil değerinin muhafazası bağlamında dikkate almak makul görünmektedir.

Hukuk Muhakemeleri Kanunu (HMK), güvenli e-imza ile imzalanan belgelerin senet hükmünde olduğunu ifade ederek, e-belgeleri kesin deliller arasında kabul etmiştir (HMK, 2011). Belgenin bu delil değeri, kimlik tespiti aracı olan e-imzanın belgedeki irade beyanını göstermesi işlevinden dolayıdır. Belgede yer alan bilginin, yani açıklanan iradenin sahibi, bu imzayla belgeyi kendisinin düzenlediğini açıklamış olur. Bundan dolayı belgenin delil değerini taşıyıp taşımaması, ağırlıklı olarak e-imzanın varlığına bağlıdır. Bu durumda belgenin geçerliliği ve özgünlüğü e-imza üzerine inşa edilmiştir. Ancak, bu durum hep böyle mi kalır, zamanla nasıl değişir, hâlâ cevap bekleyen sorulardandır. Diğer bir deyişle, zaman içerisinde e-imza geçerliliğini yitirir mi? Eğer böyle bir durum ortaya çıkarsa, hangi sonuçlarla karşılaşılacaktır? 100 yıl saklanacak e-belgedeki imza nasıl koruma altına alınacak? E-imza geçerliliğini yitirirse, belgenin delil değeri nasıl sağlanacak? İmza geçerliliğini korusa dahi, kırılgan bir yapıya sahip olan dijital ortamlarda e-belgelerin delil değerinin sürdürülmesinde hangi yöntemlerden faydalanılacak? Bu sorulara doğru cevap bulabilmek için e-imza dışında da elektronik delil elde etme yöntemleri aranması gerektiği görülmektedir.

Bu yöntemlerden birinin arşivsel bağ kurmak olduğu düşünülmektedir. Arşivsel bağ, belgenin diplomatik özelliklerinden faydalanarak belge ile üreten, üretenin bağlı olduğu müdürlük ve kurum ile muhafaza edileceği dosya arasındaki ilişki ağının açığa çıkarılması demektir. Bir belgenin ortaya çıktığı bağlam olan kontekst tespit edilerek onun özgünlüğü ve delil özelliği değerlendirilebilir. Kontekst belgenin üretilmesinden dosyalanmasına, korunmasından arşiv deposunda bulunduğu yere kadar yaşam döngüsünü açıklayabilmektir. Bu döngüde hem belgenin kendi bütünlüğü içerisinde form özellikleri hem de bulunduğu dosya ve üretildiği idari organlarla olan münasebeti sorgulanır. Böylece onun güvenilirliği pekiştirilmeye çalışılır. E-belgelerin özgünlüğü ile ilgili tartışmalar, elektronik belgelerin yaşam döngüsü içerisinde karakteristik özelliklerini kaybetme, ait olduğu dosya ve diğer belgelerle ilişkisinin kopması gibi delil değerini kaybettirebilecek ihtimallerden kaynaklanmaktadır. Bu durum, daha çok dijital ortamın güvensizliği ile yazılımdan kaynaklanabilecek problemler nedeniyle ortaya çıksa da, söz konusu ihtimallerin, belgelerin form özelliklerini kullanarak üreticisi ve aynı fonksiyon kapsamındaki diğer belgelerle olan ilişkisini tespit etmeye imkân veren arşivsel bağın tam olarak kurulamamasından dolayı oluşabileceği düşüncesini akla getirmektedir. Bir belge ve bulunduğu dosya için bu bağın kurulamamasının, belgelerin delil değerini olumsuz yönde etkileyeceği düşünülmektedir.

Bu çalışmada "elektronik delil elde etme yöntemi olarak arşivsel bağın kullanılabileceği" hipotezi savunulmaktadır. Çalışmada betimsel analiz yönteminden faydalanılmaktadır. Değerlendirilecek mevzudan dolayı, konunun bilişim, idare hukuku, hukuk muhakemeleri usulü alanıyla ilişkisi bulunmaktadır. Ancak, bahsi geçen alanlar müstakil birer inceleme konusu olduğu için ayrı ayrı çalışmalarda ele alınmasında fayda bulunmaktadır. Konu, bu çalışma kapsamında, daha çok arşivcilik ve belge yönetimi literatürü ışığında incelenecektir. Literatür incelemesi yapılırken, Türkçe ve İngilizce kaynaklar kullanılmıştır. Türkçe aramalarda "arşivsel bağ", "özgünlük", "otantiklik", "güvenilirlik", "adli bilişim", "belge-adli bilişim", "belge-üstveri", İngilizce aramalarda ise "archival bond", "authenticity", "trustworthiness", "digital record forensics", "records and (ve) forensics", "records and (ve) metadata" anahtar kelimeleri kullanılmıştır.

Çalışmanın birinci bölümünde, e-belgelerin özgünlüğünde diplomatik analiz yöntemlerinden nasıl faydalanıldığı ele alınmış ve bir üstveri alanı olarak arşivsel bağın kurulması hususundaki kanaatler tartışılmıştır. İkinci bölümde konu ile ilgili literatürdeki çalışmalar ve çeşitli projeler arşivsel bağın kurulmasına yönelik yaklaşımları açısından incelenmiştir. Üçüncü bölümde ise belge yönetiminde kullanılan elektronik delil elde etme usulleri açıklanmış, elde edilen neticelerin muhtemel çalışmalar ve sonuç kısmında değerlendirilmesine gayret edilmiştir.

E-Belgelerin Özgünlük İncelemelerinde Diplomatik ve Arşivsel Bağ

Üretildiklerinden itibaren dijital ortamda saklanan e-belgelerde, bu ortamın kırılganlığından kaynaklanan bazı sorunlarla karşılaşılmaktadır. Bu sorunlar, e-belgenin özgünlüğünü olumsuz etkileyecek niteliktedir. Söz konusu sorunların temel kaynağı, e-belgelerin saklandığı sunucu ve sabit disklerdeki bozulmalar, e-belgenin sahip olduğu formatın eskimesi, e-belgelerin yaşam döngüsünde kullanılan yazılımlar olarak belirtilmektedir (Çiçek, 2016; Valle, 2017). Bunlar, e-belgelerin özniteliklerinin korunamamasına neden olup, yaşam döngüsü içerisinde karakteristik özelliklerini kaybetme, ait olduğu dosya ve diğer belgelerle ilişkisinin kopması gibi riskler barındırmaktadır. Tüm bu olumsuzluklar, belge yöneticilerini doğrudan ilgilendiren sonuçlar olarak karşımıza çıkarmaktadır (INTERPARES, 2008a; Archives of New Zealand, 2017).

2000'li yıllardan itibaren elektronik ortamda üretilen belgelerde özgünlüğü olumsuz etkileyen sorunlarla karşılaşıldığı görülmüştür. Söz konusu sorunlar, belgenin delil değerini de etkilemektedir. Çünkü belgenin özgünlüğünün korunması, delillerin özelliklerinden olan "gerçeklik ve ispatı sağlamaya yönelik ilişkiyi gösterebilmek" anlamına gelmektedir. Bu nedenle, belge yönetimi uzmanları e-belgelerin özgünlüğünün korunmasına ciddi bir önem vermiştir. Kanada'da British Columbia Üniversitesinde Luciana Duranti'nin başkanlığında devam ettirilen INTERPARES Projesi kapsamında bu konuda önemli çalışmalar yürütülmüş olup, e-belgelerin özgünlüğünün korunmasında diplomatik analiz yönteminden faydalanıldığı görülmüştür (INTERPARES, 2008a).

Diplomatik Analiz Yöntemleri

Diplomatik analiz yöntemi, Orta Çağ'da hangi belgenin orijinal olduğunun tespiti için kullanılmaktaydı (Duranti, 1998; Çiçek, 2009). Bu dönemde yasaklayıcı ve imtiyaz veren şeklinde genellikle iki hukuki fiilin sonucu olarak belge üretilmekteyken; hukuki fiil, idari teşkilat yapısı ve ticari etkinliklerin artmasıyla 20. yüzyıl'daki diplomatik araştırmaları daha çok modern belge tipolojilerinin geliştirilmesi, belgelerin form özelliklerini kritik eden özel diplomatik yöntemlerin çeşitlendirilmesi ve arşivsel bağın kurulması üzerine gerçekleşmiştir (Çiçek, 2009; Duranti, 2010a; Rogers, 2015). Bu anlayış doğrultusunda belgeler, sadece şekil özellikleri bağlamında değil, dokümanter form, açıklama notları, taşıyıcı ortam ve kontekst unsurları kapsamında da incelenmektedir.

Kurumlarda fonksiyonların gerçekleştirilmesi için çıkarılan idari uygulamalar, belgelerin belirli standart ölçülerde üretilmesini ve türe özgü form özelliklerine sahip olmasını sağlar. İdari uygulamaları ise mevzuat şekillendirir. İdari prosedürlerin tayin ettiği bu form özellikleri, ortaya koydukları idari ve hukuki amaca göre değişmektedir. Mesela, ruhsat, sözleşme gibi kişiye tasarruf yetkisi veren belgelerle, yazışma, makbuz ve fatura gibi daha önce gerçekleşmiş fiillerin

delili olan belgelerin form özellikleri birtakım farklılıklar içermektedir. Her belge türünün farklı özellikleri o belgenin aslına ait olup, kalıtsal özelliğidir. Diplomatik uzmanları bunu dokümanter form olarak açıklamakta olup, diplomatik analizin temel unsurları arasında kabul etmişlerdir (INTERPARES, 2008b; Duranti, 2010b; Çiçek, 2012; Jansen, 2015; Rogers, 2015).

Belgenin dış kaynaklı form özelliklerinden biri olan açıklama notları belgenin üretilme sebebini açıklayabildiği için diplomatik analizin bir diğer unsurlarındandır. Açıklama notları, belgenin üretilme sebebini ortaya koymaktadır. Belgedeki mesajın taşındığı ortam ve bu ortamı tanımlayan yazı tipi, yazılış şekli, mürekkep ve mesajın iletildiği semboller taşıyıcı ortamı tanımlamaktadır. Belgenin kâğıt mı yoksa elektronik ortamda mı olup olmadığını ifade etmesi nedeniyle oldukça önemli görülüp, diplomatik analizin inceleme unsurlarındandır (INTERPARES, 2008b; Çiçek, 2009; Duranti, 2010a).

Belgeler, bürokratik bir kontekstin içerisinde üretilmektedirler. Söz konusu kontekst, işlemin yürütülüp belgenin düzenlenmesinden kimin yetkili olduğu ile belgenin muhatabının kim olduğunu açıklamaktadır. E-belgelerin diplomatik analizi söz konusu olduğunda kontekst alanındaki teknolojik kontekstin ön plana çıktığı görülmektedir (INTERPARES, 2008b). Teknolojik kontekst kritik edilirken, e-belgelerin arşivsel bağının sağlıklı bir şekilde kurulması hedeflenmektedir. Arşivsel bağ, ortamı ne olursa olsun bir belgenin üretilmesinden arşive intikal edene kadar geçen süreçte kim tarafından, hangi fonksiyon ve işlem kapsamında üretildiği, kime devredildiği, nasıl dosyalandığı ve hangi seride bulunduğu açıklanıp, bu seri içerisinde ait olduğu vaka ya da konu dosyasıyla bu dosyadaki diğer belgelerle ilişkisini kurabilmektir. Bu ilişkinin ortaya çıkarılması için dosya kodu, kişiler ve kayıt işlemleri gibi üstveriler kullanılmaktadır (Çiçek, 2011). Arşivsel bağın kurulma gereksiniminin nedeni, aynı fonksiyon kapsamında üretilen farklı tür ve formattaki belgelerin bir arada bulunması gerekliliğidir. Aksi takdirde, belgelerle üretildiği bağlam arasındaki ilişkinin kurulması pek mümkün olmaz.

Arşivsel Bağ

Aynı fonksiyon kapsamında üretilen farklı tür ve formattaki belgelerin bir konu veya vaka bağlamında bir araya getirilmesi arşivsel bağın kurulmasında önemli bir adım olarak görülmektedir (Duranti, 2010a, s. 85). Kurumlarda bir konu ya da iş bağlamında oluşan belgeler, üretildikleri bağlama göre birbirleriyle ilişkilendirilerek bir araya getirilirler (Force, 2013, s.115; Çiçek, 2015, s. 154-155). Bu noktada, belgelerle üretildikleri bağlam arasındaki entelektüel ilişkinin ortaya konulması gerekli görünmektedir. Buradaki hedef, ilgili konuda bilgi bütünlüğünün sağlanmasıdır. Belgeler, girdikleri dosyada eksik bir bilgiyi açıklamakta, dosyadaki bilgi bütünlüğüne katkı yapmaktadır. Bu nedenle, belgeler dosyalanırken önce üretildiği fonksiyonel kaynağa dikkat edilmektedir. Sonrasında, paydaşı olan diğer belgelerle olan organik bağına bakılarak belgenin

dosya bütünlüğüne yaptığı katkı değerlendirilmektedir. Böylece, dosyaya kaldırılan her belgenin diğer paydaş belgelerle bütünlük arz etmesi sağlanır. Organik bağ, belgenin kaldırıldığı dosyadaki diğer malzemeler arasında bir zincirin halkası gibi ilişki kurulmasıdır (Çiçek, 2015, s. 154-156). Bu bağ, belgelerle belgeler, belgelerle fonksiyon ve fonksiyon ile vaka arasında oluşturulacak münasebettir. Belgelerle, üretildikleri bağlam arasındaki entelektüel ilişki, belgelerin konu ya da belirli bir vaka bağlamında bir araya getirilmesiyle, yani organik bağın kurulmasıyla ortaya çıkarılmaktadır. İyi ve doğru dosyalamanın da ana temasını oluşturan bu işlem (Çiçek, 2015, s. 154), belge ile belgenin üretildiği fonksiyon arasındaki entelektüel bağı ortaya çıkararak, ilgili konudaki bilgi bütünlüğü muhafaza edilir.

Belgenin özgünlük incelemelerinde, onun ait olduğu fon, alt fon, seri ve dosyanın tespiti yapılmaktadır. Dosyaların üretildiği kaynak tespit edilerek fonksiyon ortaya çıkarılır ve dosya ile fonksiyon arasındaki organik bağ kurulur. Böylece bağlamın (kontekst) gösterilmesi hedeflenir (Jansen, 2015, s. 48). Eğer, dosyaların üretildiği kaynak tespit edilemiyor ve fonksiyon ortaya çıkarılamıyorsa fon, alt fon, seri ve dosya olarak ifade ettiğimiz belge hiyerarşisi tespit edilemediği için arşivsel bağın zarar görmüş olabileceği ihtimali üzerinde durulacaktır. Bu durum, aynı zamanda belgenin gerçekliği ile ilgili kuşkuları da gündeme getirebilir. Arşivsel bağ doğru kurulamıyorsa, o belgenin antet, imzalayan, sayı veya referans numarası gibi form özelliklerinde problem olabileceğini değerlendirmek gerekir. Böylece onun gerçekliği ve üretildiği işlem için oluşturduğu delil değeri sorgulanmaya başlanır.

Arşivsel Bağın Belge Üstverisiyle İlişkisi

Belgelerin sahip olması gereken üstveriler International Organization for Standardization (ISO) 23081 Managing Metadata for Records [Belgelerde Üstveri Yönetimi] Standardı'nda belirtilmiştir. Bu üstveriler, özgünlük, bütünlük ve gerçeklik ilişkisini de beyan eder nitelikte olmalıdır (ISO, 2006; ISO, 2009). ISO 23081, belge hiyerarşisine uygun olarak da üstverileri tasarladığı için oldukça kullanışlıdır. Çünkü belge hiyerarşisi, belgenin ait olduğu dosya ve onu üreten idari organlarla bağ kurmak anlamına gelmektedir. Buradan da belgelerin arşivlenmesinde, vazgeçilmez olan üstveri çalışmaları yapılırken, arşivsel bağının kurulmasının oldukça önemli olduğunu anlıyoruz.

E-belgelerin arşivsel bağının kurulmasında faydalanılacak üstveri elemanları dosya kodu, belgeyi üreten ve oluşturan ile ne zaman üretildiği ve arşive ne zaman devredildiği gibi bilgilerden oluşabilir. Arşivsel bağın kurulmasında söz konusu üstverilerden nasıl faydalanılacağı hususunun açıklanması gerekmektedir.

Belgenin farklı diplomatik hususiyetlerini tahlil ederek onun arşivsel bağını irdelemek; buna bağlı olarak da delil değerini sorgulamak mümkündür. Örneğin, arşivsel bağın kurulmasında önemli üstverilerden biri, belgenin kurumsal

fonksiyonlar kapsamında üretilip üretilmediğini gösteren dosya kodlarıdır. Mesela icra davaları için 641.03.03 dosya kodu kullanılsın. 2017 yılında açılmış olan bir icra davası ilgili hukuk mahkemesinden 2017/8547 nolu dava numarasını almış olsun. Burada konu numarası ve dava numarası 641.03.03[2017/8547] şeklinde birleştirilerek icra davası işlemine ait bir dosya numarasını oluşturacaktır. Bu icra davasındaki farklı tür ve formattaki tüm belgeler belirtilen numarayı alarak işlem görecektir. Böylece 2017/8547 dava numaralı icra davasıyla alakalı gelen ve giden belgeler ile aynı davayla ilişkili farklı yapıdaki materyaller belirtilen sınıflandırma numarası altında toplanarak dosyalanır. E-belgelerin arşivsel bağının kurulmasında önemli bir adımı teşkil edecek olan dosya kodundan müteşekkil olan üstveri örneğimizde 641.03.03[2017/8547] olacaktır. Böylece aynı vaka kapsamında üretilmiş farklı form ve format özelliğine sahip belgeler aynı numarayı alacaktır. Eğer bu numara olması gerektiği gibi doğru verilmişse, arşivsel bağ kurulacağı için belgenin doğru yerde ve ait olduğu fonksiyon kapsamında üretilmiş olduğu şeklinde bir değerlendirme mümkün olacaktır. Bu durum, onun delil değerinin daha güçlü savunulmasına imkan verecektir.

Belgelerin diplomatik özelliklerinin belge türüne göre farklı olabileceği kabul edilmektedir. Mesela mevzuat türü belgeler ile kartografik belgelerin, kanıtlayıcı belgelerden yazışmalar ile faturaların farklı form özellikleri bulunmaktadır. Türk Standartları Enstitüsü (TSE) Elektronik Belge ve Arşiv Yönetim Sistemi (EBAYS) 13298'de belge türü belgeye ait zorunlu bir üstveri olarak benimsenmiştir. Arşivsel bağ kurmaya yönelik yaklaşımlarda belge türüne ait üstverilerden de faydalanmanın mümkün olduğu düşünülmektedir.

Belgeyi üreten ve oluşturana ait bilgiler, belgenin dokümanter formundan anlaşılacağı için bu bilgilerden oluşturulacak üstveriler belgede kolaylıkla görülebilecektir. Belgenin ne zaman üretildiği ve arşive ne zaman devredildiği bilgilerine de kolayca erişmek mümkün görünmektedir. Bu üstverileri oluşturmak ilk başta ciddi emek istemeyen bir iş gibi gözükse de, bunları korumak noktasında çeşitli sorunların yaşandığı bilinmektedir (Yalçınkaya, 2017). Bu nedenle çeşitli ülkelerde e-belgelerde bulunması gereken zorunlu üstveriler belirlenmiştir (National Archives of Australia, 2015; Bunawan, vd. 2015; TSE, 2015). Bu üstveriler, dosya tasnif ve saklama planları, seri-alt seri, dosya ve belge düzeyindeki tanımlamalardan oluşmaktadır. Arşivsel bağın kurulması yönünde yararlanılacak belgeye ait olan belge türü, dosya kodu ve seri numarası, üretici, muhatap, üretim, kayıt ve gönderme tarihi ile e-imza bilgileri, dosyaya ait olan seri, açılış ve kapanış tarihi bilgilerinden müteşekkil olacak bir üstveri alanının tesis edilerek korunmasının daha sağlıklı sonuçlar vereceği düşünülmektedir. Bu üstveri alanının elektronik delil elde etme yöntemleriyle korunabileceği kanaatindeyiz.

Arşivsel Bağın Kurulmasına Yönelik Çalışmalar

Çeşitli ülkelerde arşivlenen e-belgelerin arşivsel bağının kurulmasına yönelik çalışmalar mevcuttur. Bu çalışmalarda genel olarak diplomatik analiz yönteminden faydalanılmıştır. Belgenin form özellikleri ve tanımlanan üstverilerinden arşivsel bağ açığa çıkarılmaya çalışılsa da, son yıllarda yapılan çalışmalarda hali hazırda kullanılan üstverilerin yeterli gelmediği ifade edilmektedir. Elektronik belge yönetim sistemlerinde (EBYS) belgeye ait üstverilerin sağlıklı korunamadığı, üstverilere erişimde sıkıntılar yaşandığı, aidiyet zincirinin kaybolduğu belirtilmektedir (Tennis, 2012; Tennis ve Rogers, 2012). Bu soruna bir çözüm olması amacıyla, INTERPARES kapsamında belgenin yaşam döngüsü boyunca güvenilirliğinin muhafaza edilmesini hedefleyen koruma zincirinin (chain of preservation) geliştirildiği görülmektedir. Bu zincirde, belgenin kurumsal fonksiyonlarla ilişkisini gösteren hususların incelenmesine gayret edilmektedir (INTERPARES, 2008a). Buradan hareketle, belgenin özgünlük incelemelerinde kullanılacak bir taksonomi (anahtar sözcük sistemi) oluşturulmuştur. Bu taksonomide ekler, belgeyi oluşturan ve üretenler, arşivsel bağ, tarih, belgedeki arşivsel muameleyi tayin eden mevzuat, form özellikleri, belgede işlem yapmaya yetkili sorumlular, belgenin bulunduğu depo, erişim ve haklar, belgenin konusu ve taşıyıcı ortam üstveri elemanları olarak belirlenmiştir (Tennis ve Rogers, 2012).

Belgenin koruma zincirindeki taksonomide önemli bir üstveri alanı olarak yer alan arşivsel bağın belgenin delil değerinin korunmasında önemli bir işleve sahip olduğu düşünülmektedir. Çünkü, arşivsel bağ doğru kurulamıyorsa belgenin gerçekliğinden ve bütünlüğünden şüphe edilecek, belgenin delil değeri sorgulanacaktır. Arşivsel bağı kurarken kritik edilen hususlardan müteşekkil olan müstakil bir arşivsel bağ üstverisinin belgenin delil değerinin korunması amacıyla kullanılabileceği düşünülmektedir. Belge yönetimindeki önemli çalışmaları bulunan Luciana Duranti de bu yaklaşımı makul bulmuştur (Duranti, 2017).

Dijital ortamın güvenli olup olmamasıyla ilgili çekinceler, elektronik ortamlardan elde edilen delillerin sahihliğini korumayı amaçlayan yöntemlerin geliştirilmesini gündeme getirmektedir. Bu yöntemler, literatürde daha çok digital forensics'in karşılığı olarak kabul edilen adli bilişim adı altında değerlendirilmektedir.

Literatür analizi kapsamında incelenen çalışmaların çoğunda, e-belge veya dosyaların tanımlanmasında müstakil olarak arşivsel bağ üstverisinin oluşturulmadığı anlaşılmaktadır. Bu yaklaşım sebebiyle arşivsel bağ üstverisinin, elektronik delil elde etme yöntemleri bağlamında değerlendirilmediği gibi bir kanaat oluşmuştur. Söz konusu çalışmalar aşağıda incelenmektedir.

Jansen, INTERPARES metodolojisini kullandığı çalışmasında klasik diplomatik analiz metodunu nesneye dayalı diplomatik analiz metoduyla harmanlamıştır. Bu metotta belgenin yanı sıra, belgenin üstverilerinin de dikkate alındığı

görülmektedir. Türü ve formatı ne olursa olsun belgenin özgünlüğüyle ilgili fikir verebilecek temel veri setlerini belirleyerek bu verileri tüm belge türleri için genişlemeye müsait bir şekilde standartlaştırmak amaçlanmaktadır. Bu veri setlerinin de EBYS'lerde bir belge kriteri olarak tasarlanması hedeflenmiştir (Jansen, 2015).

Jansen, belgenin diplomatik özelliklerinden kontekst, üretim tarihi ve üreten/oluşturan verilerinin asla değiştirilemeyecek şekilde kapsülleştirilerek belgede bir üstveri olarak korunması üzerine bir kurgu geliştirmiştir (Jansen, 2015, s. 52). Her ne kadar nasıl gerçekleştirileceği konusunda bir yöntem açıklanmamışsa da, söz konusu kurgu, e-belgelerin arşivsel bağının kurulması yönünde önemli bir yaklaşım olarak kabul edilmektedir. Elektronik delil elde etme yöntemlerinden nesneye dayalı diplomatik analizde geçerli olacak üstverilerin korunmasında faydalanılabileceği düşünülmektedir. Fakat, konuyu yeteri kadar açıklığa kavuşturmak için bu konuda daha fazla çalışmanın yapılması gerekli görülmektedir.

Hindistan Elektronik ve Bilgi Teknolojileri Bakanlığı tarafından desteklenen bir projenin çıktısında, aktif olarak kullanılan e-belgelerin uzun süreli muhafazasında karşılaşılan problemler belirtilerek, uzun süreli muhafaza için e-belgelerde bulunabilecek üstveri şemaları açıklanmıştır (Katre, 2012). Bu üstverilerde, müstakil olarak arşivsel bağ üstverisi oluşturmaya yönelik bir yaklaşımın benimsenmediği gözlenmektedir.

Norveç'te yapılan bir çalışmada e-belgelerin yaşam döngüsü içerisindeki tüm süreçlerde güvenilirliğin sorgulanabileceği bir yapının kurulduğu görülmektedir. Bu yapıda belgenin güvenilirlik sorgulamasında kullanılabilecek üstveriler belirlenerek elektronik belge yönetim sistemi (EBYS) kullanıcılarının ister belgenin üretiminden hemen sonra, isterse arşive devrinde ya da EBYS'deki kullanımı sırasında sorgulama yapabileceği bir modül geliştirilmiştir (Ma vd., 2011). Bu modülde kullanılan üstveriler, Avustralya Milli Arşivinin oluşturmuş olduğu üstveri setlerinden yararlanılarak düzenlenmiştir (National Archives of Australia, 2015). Bu üstveri setlerinin, belgeyi oluşturan ve kontekst gibi bazı diplomatik özellikleri dikkate alsa da belgenin arşivsel bağına yönelik üstverileri müstakil bir üstveri alanı olarak tasarlamayı yeteri kadar gündeme almadığı görülmektedir.

TSE 13298 EBAYS'da arşivlenen e-belgelerin güvenilirliğini ilgilendiren bütünlük, form özellikleri, onay ve kayıt bilgisi ile fonksiyonel ilişki gibi e-belgenin aidiyet zincirini ortaya çıkaracak olan unsurlar belge kriteri olarak benimsenmiş ve bunlar zorunlu üstveriler olarak kabul edilmiştir (TSE, 2015). Bu unsurlara arşivsel bağın kurulmasında oldukça dikkat edilmektedir. TSE 13298 EBAYS'da belgenin diplomatik özelliklerinden arşivsel bağın kurulmasında faydalanabileceği açıklanmış olsa da, müstakil olarak arşivsel bağ kurmaya yönelik bir üstveri alanının oluşturulmadığı görülmektedir.

Malezya'da arşivlenen e-belgelerin özgünlüğü ve devamlılığı için E-SPARK adında bir proje başlatılmıştır. Bu projenin ilk safhasında kamuda üretilen e-belgelerin yönetimiyle ilgili temel ilkeler ve süreçler ile prosedürler belirlenmiş, 2. safhasında ise arşive devredilen e-belgelerin yönetimi üzerine yoğunlaşılmış, daha çok üstverilerin korunması üzerine inşa edilecek bir yöntem kurgulanmıştır. Üstverilerin önemi ifade edilerek mevcut üstverilerin sağlanmasında karşılaşılan problemler belirtilmiş ve benimsenebilecek yöntemler açıklanmıştır. Kullanılan üstverilerin yeterli gelmediği ifade edilmiş, geliştirilen PEREHM üstveri modeli tanıtılmıştır. Bu modelde, üstverilerin belgenin oluştuğu andan itibaren belge ile birlikte hareket ederek belge arşive devredildiğinde de aidiyetinin kopmaması gerektiği ifade edilmektedir. Böylelikle bu üstverilerden belgelerin güvenilirliğinin sağlanmasında faydalanabileceği belirtilmektedir (Bunawan vd., 2015). Fakat bu modelde, belgelerin diplomatik özelliklerinden faydalanıldığı görülememiş, dolayısıyla arşivsel bağ kurmaya yönelik bir üstveri alanının kurgulanmadığı gözlenmiştir.

Norveç'de 2006-2009 yılları arasında e-belgelerin uzun süreli muhafazasında karşılaşılan problemler incelenmiştir. Proje sonunda e-belgeler için kullanılabilecek üstveri alanları oluşturulmuştur. Bu alanlarda özgünlük bilgisi ayrı bir set olarak belirlenmiş, orijinallik, erişim kontrolü ve bütünlük bu setin birer parçası olarak kurgulanmıştır (DNV, 2010). Özgünlüğün bir üstveri seti olarak kurgulanması oldukça önemli bir gelişme olarak kabul edilebilir. Belgeye ait üstverilerin kapsülleştirilerek koruma altına alındığı ve güvenilirliğin tesisinde belgenin diplomatik özelliklerinden faydalanıldığı anlaşılmaktadır. Burada arşivsel bağ kurmaya yönelik bir üstveri alanının oluşturulduğu görülmektedir.

INTERPARES araştırmaları kapsamında yapılan bir çalışmada da arşivsel bağı kurarken dikkat edilen hususlardan bir üstveri modeli oluşturulmuştur (Tennis, 2012). Söz konusu yaklaşımın, elektronik delil elde etme yöntemleriyle geliştirilebileceği düşünülmektedir. INTERPARES kapsamında yapılan araştırmalarda da bu yönde tartışmalar yapıldığı bilinmektedir (Duranti, 2017).

Belge Yönetiminde Elektronik Delil Elde Etme Yöntemleri

İdari ve hukuki işlemlerde bilişim sistemlerinin giderek artan bir şekilde kullanılmasıyla elektronik deliller gündeme gelmiş ve elektronik delillerin tespiti, muhafazası ve yargı mercilerine sunulması bir gereklilik olarak ortaya çıkmıştır (Orta, 2015, s. 128). İşte bu noktada, literatürde adli bilişim kavramıyla karşılaşmaktayız. Computer forensics ya da digital forensics olarak geçen kavram ülkemizdeki çalışmalarda daha çok adli bilişim olarak kullanılmaktadır (Orta, 2015, s. 130-139; Özen ve Özocak, 2015, s. 44). Adli bilişimin pek çok tanımı bulunmakla birlikte, elektronik ortamlarda delil elde etme amacıyla inceleme ve tetkikler yapılması olarak tanımlamak mümkündür (Orta, 2015, s. 136; Özen ve

Özocak, 2015, s. 44). Yapılan iş ve işlemlerin mahiyeti göz önüne alındığında adli bilişim kavramının muhtevasını tam olarak karşılamadığı düşünülmektedir. Bunun yerine elektronik delil elde etme teriminin daha sağlıklı olacağı kanaatindeyiz. Konu uzmanlarının da adli bilişim kavramının yeteri kadar açıklayıcı olmadığı yönünde bir yaklaşımı benimsediği görülmektedir (Aydoğan, 2009).

Elizabeth Diamond, arşivciyi belgelerin delil değerini korumayı hedefleyen bir delil elde etme yöntemleri uzmanı olarak tanımlamıştır (Diamond, 1994'dan aktaran Duranti, 2009, s. 40). Günümüzde üretilen arşiv malzemesinin büyük bir çoğunluğu ise elektronik ortamda oluşturulmaktadır. Elektronik ortamın doğasından kaynaklanan bazı sorunlarla karşılaşıldığından, arşivcilerden de kendilerini elektronik delil elde etme uzmanı olarak yetiştirmeleri beklenmektedir. E-belgelerde karşılaşılan sorunların elektronik delil elde etme yöntemleriyle çözülmesi yönünde çeşitli girişimler görülmektedir. Karşılaşılan sorunlara sabit disklerde saklanan bilgilerin kaybolma ihtimali örnek verilebilir. Bir yönüyle e-belgelerde elektronik delil elde etme yöntemleri, belgenin provenans, orijinal düzen ve aidiyet zincirini tespit etme çabasıdır. Aslında bu çaba, arşivsel bağın kurulması gayretinden başka bir şey değildir (Lee, 2012a).

Bu çabadan hareketle Duranti, elektronik delil elde etme yöntemlerinin belgenin güvenilirliğini incelemek için kullanılabileceğini ifade etmektedir (Duranti, 2009; Duranti ve Endicott-Popovsky, 2010; Xie, 2011; Duranti ve Rogers, 2013). Duranti, çalışmasında elektronik delil elde etme yöntemleriyle diplomatik analizin ortak yanlarını belirterek e-belgelerin güvenilirliğinin incelenmesi doğrultusunda birlikte değerlendirilebileceğini belirtmektedir (Duranti, 2009, s. 61-64). Fakat kullanılabilecek yöntemler hakkında açıklamaların yapılmadığı görülmektedir. Bununla birlikte, Cohen, e-belgelerin diplomatik analizinde klasik yöntemleri kullanmanın pek mümkün olmayacağını, elektronik delil elde etme yöntemlerinden faydalanmanın gerektiğini söylemektedir. Cohen, çalışmasında e-belgelerin diplomatik analizinde kullanılabilecek soruların örneğini verse de bu soruların bir saha çalışmasına dayanarak belirlendiğiyle alakalı kesin bir bilgi bulunmamaktadır. Cohen, yeni araştırmalarla elektronik delil elde etme yöntemleri kullanılarak e-belgelerin diplomatik analiz şablonu oluşabileceğini dile getirmektedir (Cohen, 2015, s. 37-42).

Dietrich ve Adelstein, dijital ortamda üretilen sanat eserlerinin bütünlüğünün korunmasında faydalanabilecek elektronik delil elde etme yöntemlerini açıklayarak arşivcilere bu yöntemler hakkında bilgiler sunmaktadır (Dietrich ve Adelstein, 2015). Milli arşivlerin de bazı uygulamalar benimsediği dikkat çekmiştir. Avustralya Milli Arşivinin kendisine devredilen e-belgeler için bir hash (iz) değeri oluşturduğu görülmektedir. Bu değer ve özet fonksiyonu bilgileri, e-belgenin zorunlu üstverileri arasında yerini almaktadır (National Archives of Australia, 2015, s. 125-126).

Majore, Yoo ve Shon, arşivlenen e-belgelere ait üstverilerin elektronik delil elde etme yöntemleriyle korunabilmesini öngören çalışmalarıyla dikkat çekmektedir. Bu projenin Güney Kore'deki bir saha çalışmasına dayandığı anlaşılmaktadır. E-belgelerin üretiminden itibaren oluşturulacak üstverilerin e-belgeden ayrı olarak saklanabileceği ifade edilmektedir. Bu üstveriler, belge sisteme kaydedildiğinde ve belgenin formatı değiştirildiğinde elde edilen ve hiç değişmeyeceği öngörülen iz değeri, zaman damgası ve belgenin bulunduğu yerin tanımlayıcısıdır (Majore, 2013, s. 192).

E-belgelerin güvenilirlik incelemesinde bazı elektronik delil elde etme tekniklerinden faydalanılmaktadır. Bunlar, kriminal uzmanları tarafından geliştirilen çeşitli yazılımları kullanma, imaj alma, yazma koruma adaptörleri kullanmak gibi temel tekniklerdir (Lee, 2012b; Woods vd., 2013). Kullanılan tekniklerdeki bazı süreçlerde sorunlarla karşılaşıldığı bilinmektedir. Karşılaşılan sorunlardan biri kullanılan yöntemler sonucunda oluşturulan belgenin iz değeridir. İz değeri oluşturulurken, eşsiz bir algoritmik kod belgeye tanımlanmaktadır. Belge ilk üretildiğinde oluşan iz değeri daha sonraki kontrollerde oluşturulan iz değeriyle örtüşmüyorsa, belgede bir değişikliğin meydana gelmiş olabileceği düşünülecektir. Belgelerin teknolojik değişimlerden etkilenmemesi için bulundukları sunucular zaman zaman yedeklenmektedir. Ayrıca, belgelerin bulunduğu sabit sürücüler zamanla bazı kayıplar yaşanmasına sebebiyet vermektedir (Valle, 2017). Bu durumda, belgenin ilk oluşturulan iz değeri, daha sonra oluşturulan değerlerle örtüşmeyebilir (Majore, 2014). Örtüşme olmadığından belgede bir değişikliğin meydana gelip gelmediği hususunda şüpheye düşmek mümkündür.

Elektronik belgelerin uzun vadeli saklanmalarında delil değerini ne kadar koruyacağı merak edilmektedir. Söz konusu değerin belgenin imhasına kadar korunması gerekmektedir. Bu amaçla, delil değerinin sürdürülmesinde diplomatik analiz ve elektronik delil elde etme yöntemlerinden faydalanıldığıyla ilgili olarak Dijital Belgelerde Delil Elde Etme Projesi (Digital Records Forensics Project [DRF]) kapsamında çeşitli araştırmalar yapılmıştır. Araştırma sonunda e-belgelerin delil değerinin sürdürülmesi için bir model geliştirilmiştir. Bu model adli soruşturmalar için kurgulanmış olsa da elektronik delil elde etme yöntemleri üzerine bina edilmiştir (Jansen, 2010; DRF, 2011; Xie, 2011). Üzerinden 6 yıl geçmiş olmasına rağmen, söz konusu modelin kullanım sahasının yeni araştırmalarla genişletilmesi, geçerlilik düzeyinin incelenmesi gerektiği ayrıca belirtilmelidir.

Teknolojik formatların eskimesinden dolayı daha önceki teknolojilerle oluşturulmuş e-belgelerin erişilememesi problemleriyle karşılaşıldığı bilinmektedir. Bu probleme karşı, elektronik delil elde etme yöntemlerinden faydalanılan çeşitli projeler gerçekleştirilmektedir. Bu projelerde format ne olursa

olsun e-belgelere erişimi mümkün kılacak yapılar üzerine araştırmalar yapıldığı gözlenmektedir (Jansen vd., 2016).

Sonuç

Elektronik ortamda üretilen belgeler uzun süreli kullanılmak istendiğinde, üretildikleri dijital ortamın kırılgan yapısından dolayı bazı sorunlarla karşılaşılmaktadır. Bu sorunlara, belgelerin yaşam döngüsü içerisinde karakteristik özelliklerini kaybetmesi, ait olduğu dosya ve diğer belgelerle ilişkisinin kopması, teknolojik göç sırasında yaşanan kayıplar, yazılımların üstverileri koruyamaması gibi hususlar örnek verilebilir. Söz konusu sorunlar, belgenin özgünlüğünü olumsuz etkileyecek niteliktedir. Bu sorunları bertaraf etmek için dijital ortamın doğasına özgü çözümler geliştirmek gerekli görülmektedir.

Hukuk ve ceza muhakemesinde kullanılmak üzere dijital ortamda üretilen verilerin delil niteliğini inceleyen yaklaşımlar bulunmaktadır. Bu yaklaşımlar, daha çok adli bilişim olarak ifade edilse de, bu kavramın söz konusu yaklaşımın mahiyetini yeteri kadar açıklayamadığını düşünmekteyiz. Bunun yerine, elektronik delil elde etme terimini kullanmayı tercih etmekteyiz.

E-belgeler de basılı belgeler gibi delil niteliği taşımaktadır. Bu delil niteliği, belgenin yaşam döngüsü boyunca korunmalıdır. E-belge, gerçeklik ve ispatı sağlamaya yönelik ilişkiyi gösterebildiği sürece delil olma özelliğini sürdürecektir. Bu özellik, e-belgelerin özgünlük incelemelerinin de amacını oluşturmaktadır. Bu noktada e-belgelerin özgünlük incelemeleriyle, delil niteliğini ortaya çıkarma çabalarının örtüştüğünü görmekteyiz.

Özgünlük incelemelerinde açığa çıkarılmak istenen arşivsel bağ, e-belgelerin delil niteliğini belirginleştiren önemli unsurlardan biridir. Aynı amaçları taşımalarından dolayı elektronik delil elde etme yöntemlerinin e-belgelerin özgünlük incelemelerinde kullanılabileceği düşünülmektedir. O halde, arşivsel bağ bir elektronik delil elde etme yöntemi olarak kullanılamaz mı sorusu akla gelmektedir. Çalışmamızda, literatürdeki kaynaklarda bu sorunun nasıl değerlendirildiği araştırılmıştır. Arşivsel bağın açığa çıkarılmasında tetkik edilen hususların müstakil bir üstveri alanı olarak kurgulanıp, bu kurgunun elektronik delil elde etme yöntemleriyle korunup korunmadığı incelenmiştir.

E-belgelerin yaşam döngüsü boyunca kullanılacak üstveriler, standartlar ya da milli arşivler tarafından belirlenmektedir. Bazı çalışmalarda arşivsel bağın açığa çıkarılmasında tetkik edilen hususların üstveri olarak benimsendiği görülse de, bu üstverilerin zorunluluk arz etmediği anlaşılmaktadır. Aynı zamanda, ikisi haricinde ele alınan diğer çalışmalarda, e-belgelerin arşivsel bağı açığa çıkarılırken incelenen hususların müstakil bir üstveri alanı olarak kurgulanmadığı

görülmüştür. Bununla birlikte, bu yönde tartışmaların yapıldığı bilinse de arşivsel bağın elektronik delil elde etme yöntemi olarak benimsendiği bir çalışma gözlenmemiştir.

Belge yönetiminde elektronik delil elde etme yöntemlerinin kullanımı giderek artmaktadır. Bu yöntemlerin e-belgelerin arşivsel bağının açığa çıkarılması yönünde kullanımına henüz yeteri kadar rastlanmasa da, önümüzdeki günlerde böyle bir yaklaşımın daha sık tartışılacağını tahmin etmekteyiz. Son zamanlarda blockchain (zarflama - blok zincir) yönteminin belge yönetimindeki kullanımı üzerine tartışmaların yapıldığını görmekteyiz. Bu yöntem, elektronik belgelerin arşivsel bağının açığa çıkarılması ve özgünlüğünün incelenmesi yönünde yeni kullanılmaya başlansa da, geniş örneklemlerde nasıl sonuçlar alınacağı şu an için bilinmemektedir. Bu husustaki incelemelerin artarak devam edeceğini tahmin etmekteyiz.

Ülkemizde, elektronik delil elde etme yöntemlerinin belge yönetiminde nasıl kullanılabileceği hususunda uygulamalı çalışmaların yapılması bir gereklilik olarak görülmektedir. Bunun için, hukuk, bilişim ve kamu yönetimi gibi farklı disiplinlerden araştırmacılarla ortak araştırmalar gerçekleştirmenin sağlıklı sonuçlar vereceğini düşünmekteyiz.

Kaynakça

Acar, A. E. (2012). *Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Niteliği*. İstanbul: On İki Levha Yayıncılık.

Archives New Zealand. *State of Government Recordkeeping 2015/16*. 2 Eylül 2017 tarihinde http://archives.govt.nz/sites/default/files/report_-_state_of_government_recordkeeping_2015-16_final.pdf adresinden erişildi.

Aydoğan, H. (2011). *Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri*. Polis Akademisi. Yayınlanmamış Yüksek Lisans Tezi.

Berkin, N. (1946). İspat Hukukunda Senet Delili ve Yazılı Şekil. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*. 12(4), 1175-1192.

Bunawan, A. vd. (2015). A Model for Preserving the Electronic Records Event History Metadata in Malaysia Government Agencies, Al-Dabass, D., Ibrahim, Z., Shapiai, M. I. (Ed.). *Seventh International Conference on Computational Intelligence, Modelling and Simulation*, *27-29 Temmuz 2015, Pahang-Malezya*. *İçinde* (ss. 29-34). *Yayın yeri yok. Institute of Electrical and Electronics Engineers*.

Ceza Muhakemesi Kanunu. Kanun No: 5271, R.G., S 25673, tar. 17.12.2004. 22 Mayıs 2017 tarihinde http://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm#1 adresinden erişildi.

Cohen, F. B. (2015). Digital Diplomatics and Forensics: Going Forward on a Global Basis, *Journal of Records Management*. 25(1), 21-44.

Çiçek, N. (2009). *Modern Belgelerin Diplomatiği*. İstanbul: Derlem Yayınları.

Çiçek, N. (2011). Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme, *Bilgi Dünyası*, 12 (1), 87-104.

Çiçek, N. (2012). Belgelerin Dokümanter Yapısı, *Arşiv Dünyası*, 13, 32-37.

Çiçek, N. (2015). *Kurumsal Bilgi ve Belge Yönetimi*. İstanbul: Marmara Belediyeler Birliği.

Çiçek, N. (2016). Belediyelerdeki Elektronik Belge Yönetimi Sistemlerinde Dijital Devamlılığı Tehdit Eden Yazılıma Dayalı Sorunlar. Bülent Yılmaz, Tolga Çakmak, Şahika Eroğlu (Yay. Haz.). *Belediyelerin Kütüphane ve Arşiv Hizmetleri Uluslararası Sempozyumu, 12-14 Mayıs 2016, Nilüfer-Bursa.* İçinde (ss.409-428). Bursa: Nilüfer Belediyesi.

Değirmenci, O. (2014). *Ceza Muhakamesinde Sayısal (Dijital) Delil*. Ankara: Seçkin Yayıncılık.

Del Valle, E. (2017). Sharing my loss to protect your data: A story of unexpected data loss and how to do real preservation. *Preservation and Archiving Special Interest Group 2017 Meeting, 11-13 Eylül 2017, Oxford-Birleşik Krallık.* 1 Ekim 2017 tarihinde https://figshare.com/articles/Sharing_my_loss_to_protect_your_data_A_story_of_unexpected_data_loss_and_how_to_do_real_preservation/5415046 adresinden erişildi.

Denham, E. (2017). *Keynote Speech in Archives and Records Association Annual Conference*. 01.09.2017 tarihinde https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/08/archives-and-records-association-annual-conference/ adresinden erişildi.

Dietrich, D. ve Adelstein, F. (2015). Archival science, digital forensics, and new media art. *Digital* Investigation, 14(1), 137-145.

Digital Records Forensics Project (2011). 2 Eylül 2017 tarihinde http://www.digitalrecordsforensics.org/ adresinden erişildi.

DNV. (2010). *Long-term Records Management*. Norveç: DNV.

Duranti, L. (1998). *Diplomatics: New Uses for an Old Science*. London: Scarecrow Press.

Duranti, L. (2009). From Digital Diplomatics to Digital Records Forensics, *Archivaria*, 68, 39-66.

Duranti, L. (2010a). Concepts and Principles for The Management of Electronic Records, or Records Management Theory Is Archival Diplomatics, *Records Management Journal*, 20 (1), 78-95.

Duranti, L. (2010b). Structural and Formal Analysis: The Contribution of Diplomatics to Archival Appraisal in the Digital Environment, Jenny, Hill (Ed.). *The Future of Archives and Recordkeeping: A Reader*. İçinde (ss. 65-88). *London: Facet*.

Duranti, L. ve Endicott-Popovsky, B. (2010). Digital Records Forensics: A New Science and Academic Program for Forensic Readiness, *Journal of Digital Forensics, Security and Law*, 5(2), 45-62.

Duranti, L. ve Rogers, C. (2013). Memory Forensics: Integrating Digital Forensics with Archival Science for Trusting Records and Data, *eForensics Magazine*, 2 (15), 96-111.

Duranti, L. ile 15.09.2017 tarihinde yapılan görüşme.

Force, D. C. (2013). *Pursuing the Usual and Ordinary Course of Business: An Exploratory Study of the Role of Recordkeeping Standards in the Use of Records as Evidence in Canada*. Yayınlanmamış Doktora Tezi. University of British Columbia The Faculty of Graduate and Postdoctoral Studies Library, Archival and Information Studies.

Henkoğlu, T. (2014). *Adli Bilişim*. İstanbul: Pusula Yayıncılık.

Hukuk Muhakemeleri Kanunu. Kanun No: 6100, R.G., S 27836, tar. 04.02.2011, (Çevrimiçi) http:// www.resmigazete.gov.tr/eskiler/2011/02/20110204.htm, 28 Eylül 2016.

International Organization of Standardization (ISO). (2006). *Managing Metadata for Records - ISO 23081-1*. Cenevre: ISO.

ISO. (2009). *Managing Metadata for Records - ISO 23081-2*. Cenevre: ISO.

International Research on Permanent Authentic Records in Electronic Systems (INTERPARES). (2008a). *INTERPARES 2: Experiential, Interactive and Dynamic Records*. 2 Eylül 2017 tarihinde http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf adresinden erişildi.

INTERPARES. (2008b). *A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records*. 2 Eylül 2017 tarihinde http://www.interpares.org/ip2/display_file.cfm?doc=ip2(pub)policy_framework_document.pdf adresinden erişildi.

Jansen, A. (2010). Digital Records Forensics: Ensuring Authenticity and Trustworthiness of Evidence Over Time, *Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, *20 Mayıs 2010, Oakland-Amerika*. *İçinde* (ss. 84-88). *Kaliforniya: Institute of Electrical and Electronics Engineers*.

Jansen, A. (2015). Object-oriented Diplomatics: Using Archival Diplomatics in Software Application Development to Support Authenticity of Digital Records, *Journal of Records Management*, 25 (1), 45-55.

Jansen, G. vd. (2016). Designing Scalable Cyberinsfracture for Metadata Extraction in Billion-Record Archives, *13th International Conference on The Preservation of Digital Objects*,177-185.

Katre, D. (2012). An Overview of Digital Preservation Considerations for Production of Preservable E-Records: An Indian E-Government Case Study, Moore, R., Ashley, K., Ross, S. (Ed.) *9th International Conference on The Preservation of Digital Objects*, 1-*5 Ekim 2012, Toronto-Kanada. İçinde* (ss. 134-141). *Toronto: Toronto Üniversitesi*.

Lee, A. C. (2012a). Digital Forensics Meets the Archivist (And They Seem to Like Each Other), *Provenance, Journal of the Society of Georgia Archivists*, 30 (1), 3-7.

Lee, A. C. (2012b). Archival Application of Digital Forensics Methods for Authenticity, Description and Access Provision. International Council of Archives [ICA] Kongresi, 20-24 Ağustos 2012, Brisbana-Avustralya. 2 Ekim 2017 tarihinde http://ica2012.ica.org/files/pdf/Full%20papers%20upload/ica12Final00290.pdf adresinden erişildi.

Ma, J. vd. (2011). A Framework for the Assessment of the Trustworthiness of Digital Records over Time, Wang, G. vd. (Ed.). *10th International Conference on Trust, Security and Privacy in Computing and Communications*, *16-18 Kasım 2011, Changsa- Çin. İçinde* (ss.738-744). *Yayın yeri yok. Institute of Electrical and Electronics Engineers*.

Majore, S. A. vd. (2013). Next Generation Electronic Record Management System based on Digital Forensics. *International Journal of Security and Its Applications*. 7(1), 189-193.

Majore, S. A. vd. (2014). Secure and Reliable Electronic Record Management System Using Digital Forensic Technologies, *The Journal of Supercomputing*, 70, 149-165.

National Archives of Australia (2015). *Australian Government Recordkeeping Metadata Standard*. 2 Eylül 2017 tarihinde http://www.naa.gov.au/Images/AGRkMS-Version-2.2-June-2015_tcm16-93990.pdf adresinden erişildi.

Orta, M. (2015). *Bilişim Suçlarında Adlî Analiz*. Selçuk Üniversitesi. Yayınlanmamış Doktora Tezi.

Özen, M. ve Ocak, G. (2015). Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134), *Ankara Barosu Dergisi*, 73, 41-78.

Rogers, C. (2015). Diplomatics of Born Digital Documents - Considering Documentary Form In A Digital Environment, *Journal of Records Management*, 25 (1), 6-20.

Stancic, H. vd. (2016). Recordkeeping in the Digital Age – Possibilities and Challenges of Using Linking Based Timestamping and Blockchain Technology to Maintain Long Term Integrity and Authenticity, *4rd Annual Conference Archives, Harmony and Friendship, Seoul, 5-7 Eylül 2016.*

Türk Standartları Enstitüsü (TSE). (2015). *Elektronik Belge ve Arşiv Yönetimi Standardı*. Ankara: TSE.

Yalçınkaya, B. ile 16.09.2017 tarihinde yapılan görüşme.

Woods, K. vd. (2013). Automated Analysis and Visualization of Disk Images and File Systems for Preservation, Archiving Conference 2013, 2-5 Nisan 2013, Washington-Amerika. *İçinde* (ss. 239-244). *Washington: Society for Imaging Science & Technology*.

Xie, S. L. (2011). Building Foundations for Digital Records Forensics: A Comparative Study of the Concept of Reproduction in Digital Records Management and Digital Forensics, *The American Archivist*. 74, 576-599.

Yargıtay 9. Ceza Dairesi. (2013). *Esas No: 2013/9110, Karar No: 2013/12351*. 2 Ekim 2017 tarihinde http://www.kazanci.com.tr/gunluk/9cd-2013-9110.htm adresinden erişildi.

Tennis, J. T. ve Rogers, C. (2012). Authenticity Metadata and the IPAM: Progress toward the InterPARES Application Profile. *Foo, S. S. B. ve Overbeek, H*. (Ed.). *International Conference on Dublin Core and Metadata Applications*, 3-*7 Eylül 2012, Kuching, Sarawak, Malaysia*. *İçinde* (ss. 38-45). 2 Ekim 2017 tarihinde http://dcpapers.dublincore.org/pubs/article/view/3662/1885 adresinden erişildi.

Tennis, J. T. (2012). Data, Documents, and Memory: A Taxonomy of Sources in Relation to Digital Preservation and Authenticity Metadata. *Duranti, L. ve Shaffer, E.* (Ed.). *The Memory of the World in the Digital Age: Digitization and Preservation*. *An International Conference on Permanent Access to Digital Documentary Heritage*, *26-28 Eylül 2012, Vancouver, British Columbia, Canada. İçinde* (ss. 933-940).

Elektronik Belge Yönetim Sistemlerinde Bilgi Yönetimi Modellemesi

Serkan MENTEŞ
T.C. Cumhurbaşkanlığı

Mutlu UYSAL
T.C. Cumhurbaşkanlığı

Mehmet Ulvi ŞİMŞEK
T.C. Cumhurbaşkanlığı

Selman SOLHAN
T.C. Cumhurbaşkanlığı

Öz

Gelişen teknolojiyle birlikte ortaya çıkan ve son yıllarda kamu kurum ve kuruluşlarının (idare) rağbet gösterdiği elektronik belge yönetim sistemleri (EBYS) birçok aşamasını tamamlamış durumdadır. İdareler iç ve dış yazışmalarını büyük oranda elektronik ortamda (e-ortam) yürütmektedir. İdarelerin elektronik ortama geçmesindeki en büyük hedef kurumsal yazışmalar ışığında kurumsal bellekleri oluşturabilmek, hafıza kayıpları yaşamamak ve en önemlisi de fiziksel ortamdaki arşiv yapısının aksine güncel belgelerin yönetimi ve bilgi yönetimi kavramını geliştirebilmektir. EBYS ile birlikte kuruma intikal eden ve kurumdan iletilen belgeler üzerinde bilgi yönetimi sağlanabilmelidir. Bu sebeple her tür belgenin gizlilik dereceleri dikkate alınmak suretiyle belirlenecek üstveri alanları ile tasnif edilmesi hedeflenmektedir. EBYS'lerde üretilen ve tasnif edilmesi düşünülen belgeler dikkate alındığında veri boyutunun petabyte seviyelerinde olacağı düşünülmektedir. Tasnifi yapılan belgelerin çeşitliliği ve miktarı göz önüne alındığında uygulama tabanlı çözümlerin yetersiz kaldığı görülmektedir. Asıl ulaşılmak istenen özet bilginin saklı kalması uygulama kullanıcılarının bilgiye ulaşmasını engellemekte ve zaman kaybına neden olmaktadır. Aynı zamanda milyonlarca belge arasından özet bilgilerin çıkarılması zaman almaktadır. Bu kapsamda EBYS'de yer alan evrakların gruplanarak özetlenmesi bilgi yönetimi açısından fayda sağlayacaktır. Özellikle belgenin kayıt aşamasında oluşturulan özet bilgiler sonrasında raporlama olarak ilgili kullanıcılara sunulmakta ve bilgiye ulaşım daha hızlı olmaktadır. Bu makalede EBYS'de yer alan evrak süreçlerinde özet bilgi oluşturma aşamaları ve faydalarına değinilecektir. Evrakların içerdiği bilgilerin kurumlarımıza sağladığı fayda ile hızlı şekilde bilginin üretilmesi ülkemizin gelişimine ve devletimizin işleyişine katkı sağlayacaktır.

Anahtar Sözcükler: *Bilgi, Bilgi Yönetimi, Kurumsal Bellek,*

Giriş

2000'li yıllarla birlikte Türkiye'de hızla yayılan e-Devlet çalışmaları arasında yer alan ve 2004 yılında çıkarılan 5070 sayılı Elektronik İmza Kanunu ile birlikte yaygınlaşan EBYS uygulamalarının kullanımında son 5 yıldır büyük bir yükseliş görülmektedir.

EBYS kullanımında görülen bu artış ile uygulamaların geliştirilmesi ihtiyacı da ortaya çıkmıştır. Elektronik ortamda yönetilebilen arşivler, daha önceleri fiziksel ortamda oluşturulmuş fakat elektronik ortama aktarılan arşiv ve arşivlik malzemelerin yönetilmesi ve erişimi gibi alanlar EBYS ile birlikte ortaya çıkan ilk geliştirme ihtiyaçları olarak değerlendirilmektedir.

Günümüzde ise hem teknolojik gelişmeler hem de idarelerin ihtiyacı doğrultusunda çok daha detaylı geliştirmeler üzerinde teoriler ortaya atılmakta olup "Big Data, Yapay Zeka, Makine Öğrenmesi" gibi kavramlar sıklıkla karşımıza çıkmaktadır. EBYS alanında sıkça kullanılan kavramlar artış gösterirken kullanılan uygulamalar ve kullanıcı yaklaşımları gözlemlendiğinde hâlâ EBYS'lerin günü kurtarmak üzerine çözümler ürettiği, geleceğe dair projelendirme ya da uygulamaların geliştirilmesi noktasında adımların projelerde kaldığı görülmektedir.

Yaklaşık 15 yıllık bir geçmişe sahip Türkiye'deki EBYS serüveninde önemli mesafelerin kat edilmiş olması uygulamaya yönelik sorunların çözülmüş ve artık uygulama içerisindeki bilgilerin yönetilebilir olması gerekmektedir. EBYS'ye geçişteki en önemli sebep arşivlerin eskisi gibi yönetilemez bir yapıda muhafaza edilmesi yerine; yönetilebilir ve analiz edilebilir bir yapıya dönüştürülmesiydi. Oysaki günümüzdeki teknoloji düşünüldüğünde oluşan belgelerin sadece arşive intikalinde değil; cari dönemlerinden itibaren değerlendirilebileceği ve kurumsal kararlara destek olabileceği aşikârdır. Bu sebeple de EBYS uygulamalarında öncelikli olarak geliştirilmesi gereken kavram "Bilgi Yönetimi" süreci olmalıdır.

Çalışmamızda bilgiyi yönetebilmek üzerine hazırladığımız ve uygulamaya aldığımız süreci anlatmaya çalışırken kullanılan yöntem, fayda alanı, çıktıların kullanımı gibi hususları detaylandırmaya çalıştık. Bu çalışma ile kurum ve kuruluşların yoğunluklu yaptıkları yazışmaları göz önüne alarak bir süreç tayin edebilmeleri ve arşive intikal edip uzun bir süre el değmeyen belge süreçlerinin yerini anında yönetilebilen ve analiz edilen belge sürecine devretmesi amaçlanmaktadır.

EBYS'den Beklentiler

İdarelerin neredeyse tamamında EBYS'ye geçiş süreci bazı ortak nedenlere dayanmaktadır. Bu nedenleri genel olarak:

- Hızlı İşlemler; belge üretimi, imza süreci, muhataba iletim ve arşivleme
- Mali Tasarruf; sarf malzemesi, gönderim ücreti vb.
- Zaman Tasarrufu; yazışma yapılan idareler arasında geçen zaman
- Mekan Tasarrufu; arşiv depoları yerine daha küçük alanda tutulabilen dijital veri alanları
- Hesap Verebilirlik; Kayıt altında yürütülen belge süreci ile her adımın hesap verebilir hale gelmesi.
- Ekolojik Kazanç; Dijital ortam ile kağıt israfının düşmesi

şeklinde sıralamak mümkündür. Bahsedilen nedenlerin birçoğu günümüzde gerçekleştirilebilmektedir. Mevzuat üzerinde yapılan düzenlemeler, memurların uygulamaya olan bakış açılarının değişmesi gibi sebeplerle birlikte artık EBYS'ler faydaları ile birlikte idarelerce benimsenmiş bulunmaktadır.

Belgenin Bilgiye Dönüşümü ve Dönüşümdeki Engeller

Belgelerin eski şartlara göre daha hızlı üretilmesi veya daha hızlı işleme alınması ve sağlanan bazı tasarruflar ile birlikte yeni idare anlayışıyla gelen ihtiyaçlar sebebiyle de EBYS'ler yaygınlaşmıştır. Yeni idare anlayışında artık iş ve işlemleri yürütmek kadar doğru işlemleri yapmak da mühimdir. Bu sebeple artık bir vatandaşın talebinin mevzuat gereği belli bir süre içerisinde (hızlıca) cevaplanmasından ziyade vatandaşın talebi, şikâyeti veya teşekkür ettiği hususun değerlendirilmesi, incelenmesi hatta sonuçlandırılması daha önemlidir. Yine idareler arası yürütülen yazışmalarda geçmişte hiç yazışma yapılmamış gibi defaatle aynı konular üzerine belli aralıklarla yazışma yapmak yerine mevzubahis sorunların EBYS üzerinde araştırılması, ilgili idare ile ilgili konu üzerine yapılan yazışmaların değerlendirilmesi ve bu şekilde yürütülen iş ve işlemler daha nitelikli olacaktır.

İdarelerin elindeki kurumsal belleği analiz edebilmesi ciddi anlamda iş yükünü ortadan kaldıracak, ülkemizin en önemli sorunlarından olan uzun bürokratik yazışma geleneğini de ciddi anlamda azaltacaktır. Şöyle ki kurumsal belleğini kullanamayan idareler her türlü iş ve işlem için sürekli yazışma yapmak zorunda kalacak; geçmiş dönemde yapmış olduğu iş süreçlerini bir köşede bekletmiş olacaktır. Oysaki EBYS ile birlikte kurumlarımızın elektronik ortama taşımış oldukları belgelerini oluştuğu anda tasnif edebilmesi, ilgili kurum ve işlemler ile bağ kurabilmesi ve istenildiği anda bu belgelerin aranarak incelenmesi, analiz edilmesi eskiye nazaran daha kolay bir işlemdir. Fiziki ortamda dosyalar içerisinde aranacak ve belki de hiç bulunamayacak belgeler elektronik ortamda doğru metotlar belirlenerek ve doğru üstveri alanları ile ilişkilendirilerek her zaman hizmete açık kalmış olacaktır.

Bilgi sistemi kavramı ile bilginin toplanması, saklanması, işlenmesi, iletilmesi ve dağıtılmasına hizmet eden teknolojiler, uygulamalar ve insan kaynakları akla gelmektedir (Anameriç, 2007, ss. 24-25). Belgenin bilgiye dönüşümü ile elde edilecek kazanımlar idarelerde görülen bazı sorunlar sebebiyle hayata geçirilememektedir. İdarelerin bilgi yönetimi kavramını işletememesindeki en önemli sebepler şöyledir:

- Fiziki Uygulamaların Devam Etmesi
- Nitelikli Personel İstihdamının Sağlanmaması
- İhtiyaçların Doğru Analiz Edilmemesi
- Yetki ve Sorumluluk Dağılımlarının Yapılmaması

Bu sebepler aynı zamanda EBYS uygulamalarının sürdürülebilirliğini de engellemektedir. Mevzuata uygun kurumsal belge süreçlerinin standardize edilmesi, uygulamaları yönetecek konumdaki personelin iş ve işlemlere hâkimiyeti, kurumsal ihtiyaçların doğru analiz edilmesi, idarelerin içlerindeki yetki dağılımını doğru yapmaları ve birimlerin görev alanları göz önüne alınarak görev dağılımı yapılması bilgi yönetimi sürecini kolaylaştıracağı gibi EBYS'nin sürdürülebilirliğine de katkı sağlayacaktır.

Cumhurbaşkanlığı Bilgi Yönetimi Modeli

İdareler, kurum içerisinde belge süreci üzerine yapacakları analiz çalışmaları ile yoğunluklu olarak yapılan yazışma alanını ortaya çıkarmalı ve bunun üzerine bilgi yönetimi sürecini yürütmelidir.

Bilgi sistemleri bilgi ve veriyi işlem sürecinden geçirerek, anlamlı çıktılara dönüştürürler (Cash, McFarlan ve McKenney, 1988, s.28). Cumhurbaşkanlığında uygulanacak Bilgi Yönetimi Modeli ile de Kamu kurum ve kuruluşları ile vatandaşlardan Cumhurbaşkanlığına gelen belgelerin ve EBYS'de üretilen belgelerin kısa bir tasnif metodu ile gruplandırılması, daha sonra istenilen verilere göre rapor oluşturulması ve istatistiksel analizler elde edilmesi sağlanmış olacaktır.

Cumhurbaşkanlığı bünyesinde yürütülen analiz çalışmaları sonucunda özellikle vatandaşlardan gelen belgelerin çok sayıda olduğu (toplam gelen belge sayısının %80'i) bu sebeple de yönetilmesi gereken bilgi kaynağının öncelikli olarak bu alan olduğu tespit edilmiştir.

Bu model ile Sayın Cumhurbaşkanımız ve Sayın Genel Sekreterimiz başta olmak üzere yöneticilerimize geniş bir bilgi kaynağı oluşturabilmek, bölgesel, il ve ilçelerde yaşanan problemlerin bütüncül olarak tespiti ile çözüm üretilebilmesi için vatandaşımızın kaleminden dökülenlerin raporlanması amaçlanmaktadır.

Bilgi yönetimi modelini örneklendirilecek olursak; Bebeklerde görülen SMA hastalığının tedavi ve ilaç ithalatı üzerine Cumhurbaşkanlığına yazılan belgeler üzerine bir sorun tespiti yapılıp sorun ile ilgili çeşitli alanlarda tarama yapılarak mağdurların tam olarak ne talep ettiği ve mağdur olan kitlenin sayısı anlaşılır. Daha sonra rapor haline getirilen bu sorunu çözüme kavuşturabilecek yöneticilere sunarak bu alanda ne gibi iyileştirmeler yapılabileceği ve vatandaş mağduriyetinin giderilmesi sağlanmış olacaktır.

İlk etapta ağırlıklı olarak vatandaşımızın yazmış olduğu belgeler üzerinden yürütülecek olan Bilgi Yönetimi çalışmasına daha sonra idarelerle yapılan yazışma süreçleri de eklenecektir. Böylelikle Cumhurbaşkanlığına iletilen ve gizlilik dereceleri bulunmayan belgelerden arşive intikalinden çok daha önce yararlanılmış olacaktır.

Cumhurbaşkanlığı Bilgi Yönetimi İçin Yapılan Çalışmalar

Bilgi yönetiminin hayata geçirilebilmesi adına ilk olarak birçok sebeple birlikte TS 13298 standardında uygun ve bütün kurumca kullanılacak bir EBYS uygulamasına geçiş çalışması yürütülmüştür. Bu sebeple ilk etapta bütün kurumu kapsayan bir analiz çalışması yürütülmüş, mevcut belge oluşumundan itibaren belge yönetim süreci incelenmiş, eksiklikler tespit edilerek giderilmeye çalışılmıştır. Akabinde yapılan analiz çalışmaları sonucu kurumsal ihtiyaçları karşılayabilecek bir EBYS uygulaması temini yapılmıştır. 2017 yılı itibariyle Sayın Genel Sekreterimizin talimatıyla EBYS kullanımı kurum genelinde yaygınlaştırılmış ve gizlilik dereceli belgeler haricinde ıslak imzalı belgeler dolaşımdan kaldırılmıştır.

EBYS kullanımından sonra hem belge hem de bilginin yönetilebilmesi ve çalışmaların görev sorumluluğunun belirlenmesi için Bilgi ve Belge Yönetimi Şube Müdürlüğü oluşturulmuş, bilgi ve belge yönetimini yürütecek uzman personel istihdam edilmiştir.

EBYS kullanan idareler arasında en sık görülen eksiklik olan Kayıtlı Elektronik Posta (KEP) üzerinden belge gönderilmesi hususunda tüm idarelere Cumhurbaşkanlığına gizlilik derecesi bulunmayan belgelerin KEP üzerinden gönderilmesi için dağıtımlı bir belge hazırlanarak gönderilmiş ve daha sonra idarelerle karşılıklı olarak KEP üzerinden yazışma süreci hız kazanmıştır. Böylelikle elektronik ortamda verinin tutulması ve hardcopy (çıktı) üzerinden işlemler yürütülmesinin önüne geçilmeye çalışılmıştır.

Birimin yürüteceği iş ve işlemler için çalışma yapılarak Yönerge hazırlanmıştır. Belge üretim ve yönetim süreçleri ile her birimde birim amirince tayin edilen birim belge yöneticisi, belge yöneticisi, sistem yöneticisi, kullanıcı gibi rollerin görev ve sorumlulukları, Bilgi Teknolojileri Başkanlığı başta olmak üzere Bilgi

ve Belge Yönetimi Şube Müdürlüğü dışında görev ve sorumluluğu bulunan birimlerin yetkileri tanımlanmıştır.

İdarelerde EBYS uygulamalarının sürdürülebilirliğinde ve bilgi yönetiminin yürütülmesinde engel teşkil eden;

- Elektronik Belgelerin Paraf Nüshası ile birlikte 2 Nüsha Olarak Üretilmesi,
- Mali Belgelerin EBYS'de Üretilmemesi,
- Özlük Dosyalarının Elektronik Ortamda Oluşturulmaması,
- İzin Alacak Personelin İzin Belgesinde İmzasının Bulunması Zorunluluğu,

gibi hususlara Yönerge'de yer verilerek nasıl uygulanacağı hususu hüküm altına alınmış ve idarelerde yaşanan bu ortak sıkıntıların çözümü için çeşitli çalışmalar yapılmış ve toplantılar gerçekleştirilmiştir. Örneğin; elektronik belgelerin paraf nüshası ile birlikte 2 nüsha olarak üretilmesi hususu Yönerge'de üretilen her belgenin uygulama üzerinde 2 ayrı nüsha olarak değil, tek bir nüsha olarak tutulması şeklinde maddelendirilmiştir. Bununla birlikte Başbakanlık İdareyi Geliştirme Başkanlığı, Cumhurbaşkanlığının teklifi üzerine tertip ettiği bir toplantıyla bu hususu ilgili idareleri de çağırarak görüşmüş ve e-ortamda paraf nüshasının kaldırılabileceği konusunda görüş birliği oluşmuştur.

EBYS uygulamalarında 2 nüsha yerine tek bir nüsha tutulması ile aşağıda yer alan kazanımlar sağlanmaktadır:

- Genel itibariyle veri boyutu düşünüldüğünde veri tabanının şişmesine sebep olan paraf nüshasının kaldırılması ile veri tabanı performansının artması ve uygulamanın hızlanması sağlanacaktır.
- Veri boyutunun azalması ile birlikte belge arama sonuçlarının daha erken alınması sağlanacaktır.
- Belge e-imza süresinde tek nüsha için imzalama işlemi gerçekleşeceğinden imza süresinde önemli bir düşüş sağlanacaktır.
- Zaman damgası kullanımında tasarruf sağlanacaktır.
- Mobil EBYS kullanımında imzalama işlemi süresi yarı yarıya azalacaktır.
- Büyük ölçüde fiziksel ortamdan esinlenilerek tasarlanan dış suret ve iç suret (paraflı nüsha) yapısı elektronik ortama uygun hale getirilerek tek bir suret ile paraflar belge iz kayıtlarından takip edilir hale getirilmiş olacaktır.

- Örneğin yıllık 3 milyon belge üreten bir kurumda;

  a. Yıllık kullanılan disk miktarının yarı yarıya azalması ile yaklaşık 300.000 TL'lik bir tasarruf,

  b. Aynı verinin yedeklenmesi için kullanılan disk alanın yarı yarıya azaltılması ile 150.000 TL'lik bir tasarruf,

  c. Veri boyutunun azaltılması sonucunda veri tabanı sunucularındaki işlem yükünün azaltılması ile sunucu kaynakları ve lisans maliyetlerinde yaklaşık 50.000 TL'lik bir tasarruf elde edilmektedir.

Belgeler üzerinde yer alan bilgilerin işlenebilmesi ve maksimum fayda sağlanması için analiz çalışmaları yürütülmüş ve İhtiyaçlar, Konu Başlıkları, Yöntem ve Süreç, Ara Yüz gibi konular üzerine hem ilgili birimler hem de yüklenici firma ile geliştirme toplantıları düzenlenmiştir.

Cumhurbaşkanlığı Türkiye Bilgi Hazinesi

Bilgi yönetimi için yürütülen analiz çalışmalarında ortaya çıkan sonuç yukarıda da bahsedildiği üzere vatandaştan gelen talep, istek, şikâyet; teşekkür, tebrik davetiyenin gelen belgeler arasında büyük bir yer tuttuğu olmuştur. Bu sebeple ilk etapta vatandaşımızın kaleme aldığı bilgiyi yönetmek üzere süreç hazırlanmaya başlanmıştır. Vatandaşımızın sorunları önündeki en büyük engel olan bürokratik yazışma sürecinin kısaltılması ve yöneticilerimizin ülkemizde yaşanan sorunları ilk ağızdan bilmesi, bu çalışmanın hayata geçmesinde önemli bir yer teşkil etmektedir.

Vatandaştan gelen belgeler sisteme işlenirken aynı zamanda belirlenen üstveri alanlarıyla "Türkiye Bilgi Hazinesi" uygulamasına da işlenmiş olacak ve uygulama içerisine aktarılan belgelerle önümüze Türkiye'nin analiz haritası gelmiş olacaktır. Uygulamada tasnif unsurunu sağlayacak üstveri alanları şöyledir:

- Konum Bilgisi (Sorun Yaşanan Konum)
- Çözüm Üretecek Olan İlgili Kurum ve Kuruluş Bilgisi
- SDP Konusu (Talep – Şikâyet – Tebrik – Davetiye)
- Yapılan Analizlerle Belirlediğimiz 10 Konu Başlığından Uygun Olanı (Eğitim – Sağlık – Sosyal Güvence ve Personel Alımı – Sosyal-Kültürel – Çevre/Tarım vb.)
- Şahıs Bilgileri (Başvuran Gerçek Kişi İse)
- Özet (Daha Önce Belirlenen Asgari Kriterleri İçeren Bilgi)

Verileri uygulamaya işlenen belgeler bir üst kontrol işleminden geçerek doğru üstveri alanları ile eşleşip eşleşmediği incelenecektir. Belgelerin uygulamaya işlenmesi ile birlikte kullanıcılar Türkiye haritası ara yüzüne sahip uygulama ekranında il, bölge, yurtdışı ve yer bilgisi bulunmayanlar için diğer seçenekleri üzerinde ne kadar belge geldiği ve hangi sorunla ilgili olduğunu görebilirken aynı zamanda girilen bütün üstveri alanlarına göre de arama yapabilecektir. Örneğin; kullanıcı Manisa ilinden gelen 50678 talebin ilçelere dağılımı ile eğitim – sağlık gibi konu başlıklarından hangisini ilgilendirdiği ve eğitim konusunda Manisa ilinden gelen belge sayısını da öğrenebilecektir. Bununla birlikte daha özele inildiğinde belge oluşturan kişi, konu bilgisi ile birlikte belge önizlemesi de yapılabilecek olup Manisa ilinden 50 yaş üzeri vatandaşın sağlık alanında yazmış olduğu belgeler denildiğinde daha dar bir araştırma alanı da oluşturulabilecektir.

Kullanıcı ara yüzünde yer alan Türkiye haritasında iller arasında gelen belge yoğunluğu nüfus-yüz ölçümü oranı da dikkate alınarak açıktan koyuya doğru bir renk skalası içerisinde sunulacaktır. Yani İstanbul'dan gelen 100.000 belge ile Manisa'dan gelen aynı sayıdaki belge yoğunluğu aynı renklerde değil, İstanbul açık tondayken Manisa koyu tonlara sahip olacaktır.

Uygulama üzerinde sisteme işlenen verilerin görüntülenmesi ve belgelerin önizlemesinin yapılabilmesi ile birlikte belli periyotları içeren analizler ve istatistiksel bilgilerin de elde edilmesi mümkün olacaktır. Yani Manisa ilinde son 3 ayda artış gösteren konu, son 1 ayda hangi ilçeden belge gönderiminde artış olduğu ve hangi alanda olduğu; belli bir bölgede belli bir tarih aralığında konular arasındaki artış azalış değerlerini gösteren grafikler elde edilebilecektir.

Sistemde uzmanlar tarafından bölgesel ve konu bazlı tespitler yapılabileceği gibi yöneticilerin talimatları doğrultusunda belli konular ya da belli bölgeler üzerine de konu analizleri yapılabilecektir.

Cumhurbaşkanlığı Türkiye Bilgi Hazinesi için oluşturulan proje takvimine göre süreç üç döneme ayrılmaktadır:

- Kısa Vade (2 Ay)
    - Projenin teknik altyapısı ve gereksinimleri tamamlanacak.
- Orta Vade (Yüklenici firma ile belirlenecek)
    - Veri girişleri üzerinde kontrol mekanizmaları oluşturulacak.
    - Kurumsal uygulamalar ile entegrasyon kurulacak.
    - Bölgesel ve istatiksel olarak konu analizleri yapılacak.
- Uzun Vade (Yüklenici firma ile belirlenecek)
    - Raporlama geliştirilecek. (Belli periyotlar arasında konusal artışlar, bölgelere göre artış gösteren sorunlar, değişim grafikleri vb.)
    - İş takip sistemi oluşturulacak.

Cumhurbaşkanlığı Türkiye Bilgi Hazinesi'nin proje takvimi tamamlandığında her projede olduğu gibi öngörülemeyen geliştirmeler muhakkak ki talep edilecek ve proje daha da kapsamlı bir hal alacaktır. Proje süreci ile ilgili bir öngörü olarak; şu an için uzmanlar marifetiyle yürütülmesi planlanan tespit ve raporlama süreci danışmanlar seviyesine yükseltilecektir.

Proje tamamlandığında Türkiye'ye dair bölgesel, il ve ilçe istatistikleri, bütüncül sorun analizleri, yurtdışı taleplerinin değerlendirilmesi ve üstveri olarak girilen her alandan istekler doğrultusunda grafikler oluşturulması beklenmektedir. Örneğin;

- Yurtdışından gelen taleplerin yüzdesel olarak gurbetçi vatandaşlar ile yabancı uyruklu şahıslar arasındaki dağılımı,
- Gurbetçilerimizin veya yabancı uyruklu şahısların ağırlıklı olarak hangi konuda talepleri olduğu,
- Talepte bulunan gurbetçi vatandaşlarımızın yaş aralığı yoğunlukları
- Belirli yaş aralıklarındaki (18 – 35, 50 – 70) gurbetçi vatandaşlarımızın ağırlıklı talep ettikleri konu yoğunluğu
- Taleplerin çözüm merci olarak Türk makamları ile Yabancı Makamlar arasındaki dağılım
- Gurbetçi Vatandaşlarımızın Türk Makamlarından hangi alanda talepleri olduğu
- Yabancı uyruklu şahısların teşekkür, şikâyet, istek ve talep yazılarının yoğunluğu

gibi çoğaltabileceğimiz birçok şekilde grafik bilgisi ve raporlar oluşturulması hedeflenmektedir.

Günümüzde vatandaş taleplerinin çözümü için ilgili idarelere sevk edilen belge sürecinin yanında her idarede ve illerde temsilciler marifetiyle talepler için çözüm üretme süreci de bir diğer önemli hedeftir. Böylelikle bir idare hakkında şikâyeti ya da idareden talebi olan bir vatandaşın kaleme aldığı yazı çözüm umduğu Cumhurbaşkanlığınca sağlanmış olacaktır. Bunun yanı sıra talepler ile il ve ilçelerde yer alan idarelerle ilgili de memnuniyet analizi ortaya çıkarılmış olacaktır.

Sonuç

EBYS uygulamalarının çokça konuşulduğu günümüzde artık uygulamaların geliştirilmesi ve ihtiyaçlara göre büyümesi gerekmektedir. İdarelerin ihtiyaçları, iş ve işlemleri, bilgi kaynağının yoğunluk alanları analiz edilerek gelişen teknolojinin de yardımıyla artık sadece hızlıca belge üretip gönderme ve saklama işlemlerinden öte süreçler yürütülmelidir.

Cumhurbaşkanlığı bünyesinde EBYS ile aynı anda ortaya koyulan bilgi yönetimi sürecini anlatmaya çalışırken aslında idarelerin de belgeleri onlarca yıl sonra araştırmacılar tarafından değerlendirilecek materyal muamelesi yapmasından ziyade günümüzde yorumlanabileceği bir platform oluşturabileceklerini anlatmaya çalıştık. Böylelikle hem iş gücü anlamında hem de çalışmaların nitelik kazanması açısından önemli geri dönüşler sağlanmış olacaktır. Bununla birlikte bilgi yönetimi ile kurumsal hafızanızı canlı tutmak yöneticilerin bu hafızayı kullanabilmesini sağlayacak ve önemli kararlarda kurumsal hafızanın desteği olacaktır.

Bilgi yönetimi ile Cumhurbaşkanlığına gelen belgelerin bürokratik süreçlere dâhil edilmesini beklemek yerine farklı bir alandan yönetimi sağlanarak toplumun sorunlarının daha hızlı çözülebilmesi, derin bürokrasi içerisinde kaybolmasını önlemiş olacaktır. Aynı zamanda kurumsal olarak ihtiyacımız olan Türkiye'nin anlık ve periyodik olarak durum analizleri elde edilmiş olacaktır.

Kaynakça

Anameriç, H. (2007). Bilgi sistemleri. H.Odabaş ve H. Anameriç (Yay.Haz.). Bilgi içinde (ss.23-44). Ankara: Referans Yayınevi.

Başbakanlık. (2015). Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik.18 Eylül 2017 tarihinde http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2015/02/20150202.htm&main=http://www.resmigazete.gov.tr/eskiler/2015/02/20150202.htm web adresinden erişildi.

Cash, J. I., McFarlan, F. W. ve McKenney, J. L. (1988). Corporate information systems management: The issues facing senior executives (2.bs.). Homewood, Illinois: Dow Jones-Irwin.

Elektronik İmza Kanunu. (2004). T.C. Resmi Gazete. 25355. 23 Ocak 2014.

Türk Standartları Enstitüsü. (2007). TS 15489 Belge Yönetimi Standardı. 1-2. Ankara

Türk Standartları Enstitüsü. (2016). TS 13298/T1 Elektronik Belge ve Arşiv Yönetim Sistemi Standardı. Ankara.

Kamu Kurum ve Kuruluşlarında EBYS'nin Durumu

Hakan DEDE
Başbakanlık Devlet Arşivleri Genel Müdürlüğü

Ahmet AKBAYIR
Başbakanlık Devlet Arşivleri Genel Müdürlüğü

Öz

Bilişim teknolojilerindeki gelişmelerin kamu kurum ve kuruluşlarının iş ve işlemlerinde ve hizmet süreçlerinde kullanılmasıyla beraber "e-devlet" ve "e-kurum" gibi eylem planlarıyla kamuda EBYS kullanımı yaygınlık kazanmaya başlamıştır. Günümüzde Üniversiteler ve Belediyeler de dâhil olmak üzere kamuda elektronik belge üretimi ve kullanımı çok yaygınlaşmıştır. Bu çerçevede EBYS kullanan kurumların oranı %90'u geçmiştir.. Gelişmelerle birlikte kamu kurum ve kuruluşları fonksiyonları itibariyle iş ve işlemleri sonucunda üretmiş oldukları belgeleri diğer kurumlarla elektronik ortamda paylaşmaya da başlamıştır. Elektronik belgenin etkinliğinin artmasıyla kurumsal belleklerin, milli hafızanın ve e-arşivin önemi artmış bununla beraber arşivin ve arşivcinin niteliği de büyük ölçüde değişmeye başlamıştır. Bu aşamada klasik arşivciliğin bilgi birikiminin ve deneyiminin bilişim uzmanları ile ortak çalışmalarla elektronik ortama tam anlamıyla uyarlanması titizlikle üzerinde durulması gereken bir durum olmuştur. EBYS ile ortaya çıkan belge yöneticileri klasik arşivciliğin gerektirdiği bütün süreçleri elektronik ortamda da yönetebiliyor olmalıdır**.** Elektronik ortama geçişte Arşiv Yönetim Sistemlerinin TS 13298'in revize edilmiş 2015 yılında eklenen Elektronik Arşivleme Sistemi Referans Modeli (ELAS/RM) ile entegre çalışabilmesi, elektronik ortamda üretilmiş belgelerin ve kayıtların özgünlüğünün korunarak bu sistemlere aktarımı ve yönetimi kamuda arşivciliğin elektronik ortama taşınmasının da önünü açmıştır. İlerleyen zamanlarda da e-arşivcilerin arşiv iş ve işlemlerinin bütün gerekliliklerini elektronik ortamda yerine getirmeleri gerekecektir. Devlet Arşivleri Genel Müdürlüğü milli hafızanın geleceğe aktarılması sorumluluğuyla kamu kurum ve kuruluşlarında yaptığı denetim, eğitim ve rehberlik faaliyetleriyle elektronik ortamda arşivlemenin önemi konusuna öncelikle farkındalık yaratma gayesindedir. 2008/16 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının kullanmakta oldukları EBYS yazılımlarında TS 13298 Standardına uyumluluk şartı aranmakta ve Devlet Arşivleri Genel Müdürlüğü tarafından yürütülen denetim faaliyetleri ile uygulama hataları ve arşiv gereksinimleri incelenmektedir.

***Anahtar Sözcükler**: Milli Hafıza, E-Arşiv, Klasik Arşivcilik, E-Arşivci, Elektronik Arşivleme Sistemi Referans Modeli (ELAS/RM),*

Giriş

Elektronik Belge Yönetimi kurumların fonksiyonları sonucunda elektronik ortamda üretilen her türlü bilgi ve belgenin özgünlüğünü korumak kaydıyla üretilip işleme alınmasından paylaşımına, depolanmasına, transfer edilmesine, tasfiyesine, arşivlenmesine ve araştırma hizmetine sunulmasına kadarki sürecin eksiksiz olarak yürütülmesi anlamına gelmektedir. Bunun için her kamu kurum ve kuruluşunun kendi fonksiyon ve ihtiyaçlarını elektronik ortamlarda uygulamaya alırken arşivciliğin temel disiplininden uzaklaşmamaları belge yönetimi açısından en önemli gereksinimdir. Günümüzde klasik arşivlerini tam anlamıyla yönetemeyen kurumların ilerleyen zamanlarda elektronik ortamda daha fazla zorluk çekecekleri de aşikârdır. EBYS'de belge üretildikten sonra klasik arşivcilikte olduğu gibi belli başlı süreçlerden geçilmektedir. Bu süreçlerin sonunda ayıklama ve imha komisyonunun teşkili ve sistemden belgelerin envanterlerinin çıkarılması ve tasfiye edilmesiyle beraber arşiv yönetim sistemlerinde muhafazası gibi süreçler devam etmektedir. Bütün bu süreçleri kontrol altında tutmak kurumsal organizasyon ile gerçekleşecek bir çalışma sonucunda ortaya çıkabilir. Sorunsuz ve bütün standartlara uygun bir yazılım kullanılması halinde bile bu süreçler sekteye uğrayabilmekte belge üreticilerinin hataları da süreç yönetimini engelleyecek, aksatacak durumları ortaya çıkarmaktadır.

Kamuda elektronik belgeyle beraber kullanıcıların önemi, niteliği daha da ön plana çıkmıştır. Klasik ortamda yanlış kodla bile üretilen bir belge doğru dosyalandığı sürece dosya bütünlüğü sağlanarak kurumsal işleyişi çok olumsuz etkilememekteydi. Birim arşivlerinde saklama sürelerini dolduran klasörlerin kurum arşivine düzensiz veya düzenli bir şekilde devredilmesinden sonraki bütün süreçleri kurum arşiv sorumluları yerine getirmekteydi. EBYS ile birlikte bu sistem değişikliğe uğramış durumdadır. Belge üretildiği andan itibaren Standart Dosya Planı ve birtakım üst veri unsurlarıyla tanımlanarak sistemde tasnif edilmekte ve gerektiği takdirde bu kodlar veya özel dosyalardan erişim sağlanmaktadır. Bu durumda belge üreticilerinin ilk andan itibaren belgenin akıbetini tayin etmekle beraber sistemde nasıl bir işleme tabi tutulacağını da belirlemekte ve dosyalama işlemini yerine getirmektedir. İleride arşiv iş ve işlemlerinde aksaklıklar meydana gelmemesi için personelin arşivcilik ve dosya tasnif planları konusunda muhakkak gerekli eğitim ve farkındalık çalışmalarının yapılması gerekmektedir.

Kamu Kurum ve Kuruluşlarında EBYS’nin Yapılandırılması

EBYS’ye geçiş aşamasında kamu kurum ve kuruluşları sistemde aktif rol oynayacak kullanıcı grupları, rolleri, yetkilendirmeleri, yetki grupları, belge türleri, belge grupları ve üst veri alanlarını belirleyecek geniş kapsamlı bir proje

ekibi oluşturmalıdır. Proje ekibinde belge yönetimi, arşiv ve bilişim uzmanı gibi konusunda bilgili kişiler olmak zorundadır. Bütün kurumsal ihtiyaçlar belirlendikten sonra yazılım temin edilip geniş çaplı değerlendirme yapılarak talep edilen veya ileride doğabilecek müdahaleler için güncelleme ve kurum personelinin yazılımdaki müdahale alanları netleştirilmelidir. En ufak bir ihtiyaç ve SDP revizyonu veya kod kısıtlaması için güncelleme talep edilmeyip kurum personeli tarafından gerekli işlemlerin yapılabilmesi sağlanmalıdır.

Elektronik Belge Yönetim Sistemlerinde her kurum işleyişine ve yönetimine uygun biçimde arşivcilik prensipleri doğrultusunda yapılandırmaya ihtiyaç duymaktadır. Bilgi işlem birimleri kurumların bilişimle ilgili donanımsal ve yazılımsal unsurların kontrol merkezi olmasından ötürü EBYS'nin yükünün Bilgi İşlem Birimlerine yüklenmemesi, görev dağılımlarının doğru yapılması, bilgi işlem ve belge yönetimi (evrak/arşiv) birimlerinin koordineli olarak hareket etmesi gerekmektedir. Bu anlamda sistem yöneticilerinin sistemde teknik destek sağlayıcısı olarak bilgi işlem safhasında görevlendirilmesi, kurum belge yöneticilerinin ise klasik arşivcilikte olduğu gibi belge ve arşivcilik konusunda bilgi ve tecrübeye sahip kişilerden seçilmesi gerekmektedir. Kurum belge yöneticileri ile birlikte her birimde görevlendirilen birim belge yöneticileri bütün süreçlerde aktif rol alarak elektronik ortamda arşiv iş ve işlemlerini, süreçlerini ve birimlerin ihtiyaçlarını tespit etmelidir. Birim belge yöneticileri vasıtasıyla karşılaşılan sıkıntılar veya kurumsal ihtiyaçlar kurum belge yöneticisine iletilerek çözüm aranmalıdır. Bu aşamada kurum belge yöneticileri arşiv faaliyetleri çerçevesinde tüm talep ve ihtiyaçlarını sistem yöneticisinden destek alarak EBYS'ye yansıtmalıdır.

EBYS'nin sürdürülebilirliğini sağlamak ve bu programlardan kurumsal beklentilerin karşılanabilmesi için en az Bilgi İşlem kadar Genel Evrak, Haberleşme, Arşiv, Strateji Geliştirme, Yazı İşleri ya da kurumlarda bu birimlerin muadili olan birimlerin sorumlulukları paylaşması gerekmektedir. Kurumlarda resmi yazışmalarda uygulanacak usul ve esaslar, Standart Dosya Planında gerçekleşen revizyonlar ve dosya tasnif planlarının işleyişi, kurumsal iş akışları gibi unsurların yönetimi tek başına Bilgi İşlem tarafından gerçekleştirilemeyeceği gibi Bilgi İşlem birimlerinden böyle bir sorumluluğu sahiplenmelerini beklemek yanlış olacaktır. Arşiv Birimleri (ya da bazı kurumlarda bu görevi yürüten Yazı İşleri, Haberleşme, Genel Evrak birimleri) ve Strateji Geliştirme Birimleri (Araştırma, Planlama ve Koordinasyon) kurumların fiziksel ortamda belge yönetim sürecini yürüten birimlerdir. Elektronik ortamda bu iki birime bir de teknik ve süreç yönetimini sağlaması bakımından Bilgi İşlem birimi destek birimi olarak eklenmelidir. Çünkü bir belgenin ne kadar süre ile saklanması gerektiği, Resmi Yazışma Usul ve Esaslarına ve ilgili diğer mevzuatlara göre hangi gizlilik derecesinde olması gerektiği, belgelerin ayıklama ve imha süreçlerinin gerçekleştirilmesi gibi görev ve yetkiler arşiv ya da muadil birimlere görev olarak verilmiştir. Belgenin üretim platformu ne kadar değişirse değişsin sorumluluklar

klasik arşivcilikte olduğundan çok farklı değildir. Sadece birimler arası diyalog ve koordine arttırılarak elektronik ortamda da faaliyetlere devam edilmelidir.

Strateji Geliştirme ve muadili birimlerin 2005/7 Standart Dosya Planı Genelgesi ile sorumlu olduğu SDP ile ilgili çalışmalarda aktif olarak rol alması; SDP revizyonu, SDP ve Vaka Dosyalarının kullanımı konusunda söz sahibi olması gerekmektedir. Birimlerin ihtiyaçları doğrultusunda SDP revizyonu gerektiğinde Devlet Arşivleri Genel Müdürlüğünün onayı ile gerekli işlemleri yerine getirmekle beraber personelin SDP konusunda eğitimine de önem vermesi en önemli ihtiyaçtır.

Kamu Kurum ve Kuruluşlarında EBYS'de Arşiv Faaliyetlerinin Durumu

Kamu kurum ve kuruluşlarında üretilen belgeler birer bilgi kaynağı olarak kullanılmaktan ziyade genellikle depolarda çürüyen yığınlar olarak karşımıza çıkmaktadır. Bu yığınlar içerisinden bir evrak ihtiyacı olduğunda ise samanlıkta iğne arama faslına geçilmektedir. EBYS'de de rastladığımız bu durum üretilen bir belgeye belgenin üretiminden örneğin henüz iki ay gibi bir süre geçmesine rağmen erişilememesi veya uzun süre aranması sonucu ancak bulunabilmesi çok sıkıntılı süreçleri de beraberinde getirmektedir.

EBYS'de belge bazında en önemli unsur dosya tasnif planlarıdır. En başından dosya kodunun hatalı olarak belgeye atanması, sistemdeki bütün süreçleri olumsuz yönde etkileyecektir. SDP kodları ile beraber belgeye atanan saklama süresi, tasfiye işlem tanımı ve saklama kriterleri ile belge sistemde hem tasnif edilip sınıflandırılmakta, dosyalanmakta, klasörlenmekte hem de belgelere erişim açısından en önemli arama kriteri olarak da karşımıza çıkmaktadır.

Kamu kurum ve kuruluşlarında en önemli karşılaşılan sorun SDP'nın sisteme aktarılırken yapılan hatalardır. Bütün yapılandırmalar yapılmış kurumsal fonksiyonlar EBYS üzerinde karşılık bulmuşken belge bazında en önemli husus olan SDP konusunda bu hassasiyetin gösterilmediği fark edilmiştir. Öncelikli olarak SDP'nın kullanıcılara sunulmadan önce eksiksiz ve dinamiklerine uygun bir şekilde sisteme yüklenmesi gerekmektedir. Genellikle SDP'nin açıklama kısımlarının dikkate alınmadan sisteme aktarılmasından kaynaklanan sıkıntıların başında Genel konu başlıkları ile alt kırılımı olan SDP konu kodlarının pasifize edilmeyerek belge üzerine atanabilmesi gelmektedir. Genel Konu kodları, birer başlık olmaları sebebiyle bu kodlara Tasfiye İşlem Tanımları (Transfer - Sürekli Saklama - İmha - Değerlendirme) ve Saklama Süreleri tanımlanmamıştır. Bu yüzden farklı konu kodlarına sahip belgelerin buralarda birikmesi dosyalama hatalarının başında gelmektedir. Aynı şekilde 020 Olur/Onaylar kodunun da ilk kod olarak seçilebilmesi belge üreticilerini her türden olurların bu kodla alınması hatasına düşürebilmektedir. Sistemde kullanılmaması gereken SDP kodları pasifize edilip gerekli mantıksal uyarı mesajları ile kullanıcılar uyarıldığında

doğru kodu bulma konusunda bir adım daha kat etmiş olacaklardır. SDP kodu kullanımında bir başka hata ise kuruma gelen belgelerin aynı kodlarla kodlanarak sistemde tutulmasıdır. Bir diğer kurumdan ana hizmet faaliyetleri veya ortak alanlara ait SDP kodlarıyla kodlanmış bir belge geldiğinde belge ulaştığı kurumda da aynı konu koduna sahip olamayabilir. Belgenin gönderildiği yani alıcı kurumda hangi işi ifade ediyorsa o kodun bulunduğu klasör kodu atanması hem dosyalama hem de arşivleme açısından önem arzetmektedir. Genellikle bu durum kurumların genel evrak birimlerinde karşımıza çıkmaktadır. Gelen evrak birimlerinin kurumun her faaliyetine hâkim olmaları beklenemediğinden gelen evrakın ilgili birimlere havalesi yapıldıktan sonra buralarda SDP kodlarıyla eşleştirilip dosyalanması daha doğru olacaktır.

Bazı kurumlarda sistemde çoklu kodlama imkânı kullanıcıya sunulmazken bazı kurumlarda sistemde mevcut olmasına rağmen kullanıcı tarafından tercih edilmemektedir. Belge üreticileri birçok faaliyeti ilgilendiren belge türlerinde çoklu SDP kodu kullanma konusunda hassasiyet göstermemektedirler. Klasik arşivin de gerekliliklerinden olan belgenin fotokopisini çekip bir diğer ilgili dosyaya takma işlemini elektronik ortamda kullanmamak dosyalama zafiyeti olarak karşımıza çıkmaktadır. Bunun dışında belge üreticileri konu kodu bulamadıklarında veya geçiştirmek maksatlı sıklıkla 99 “Diğer” ve her bölüm sonunda bulunan (Örn: 929 Personelle ilgili Diğer İşler) “Diğer” kodlarıyla birimin her türden yazışmalarını kodlamaktadırlar. Böylece fiziki ortamda oluşturulan muhtelif, gelen-giden vb. türden dosyalama hatasından elektronik ortamda da kurtulamadığımız ortaya çıkmaktadır. Her türden farklı konudaki belgeler Saklama sürelerindeki ve Tasfiye işlem tanımındaki farklılıklar dikkate alınmadan sistemde dosyalanmakta bu da ileride yapılacak ayıklama imha işlemlerinde oldukça önemli bir sıkıntı yaratma tehlikesi barındırmaktadır.

Standart Dosya Planından kaynaklanan bu durumların önüne geçilmesi için en önemli adım ilk aşamada SDP’nin sisteme eksiksiz ve bütün gereklilikleri karşılayacak düzeyde aktarılması ve yapılmış olan revizyonların dikkate alınması gerekmektedir. Bununla beraber personele SDP konusunda gerekli eğitimlerin sağlanarak birim belge yöneticilerinin de belli periyotlarla kendi birimindeki yazışmaları takip ederek klasör taşıma işlemleri ile ilgili hataları düzeltmelidir. Birime yeni bir kod ihtiyacı doğduğunda ise bunu SDP’den sorumlu birime bildirerek gerekli işlemleri başlatmalıdır. Ünite amirleri belgeleri paraflarken veya imzalarken SDP işlemlerini kontrol etmeli yapılan hataları fark ederek belgeyi üreticisine iade etmeli, böylece hatalı işlemin önüne geçilmesi sağlanmalıdır. SDP konusunda yapılan hataların kullanıcı tarafından önüne geçilmesi için her kullanıcının biriminden sıklıkla çıkan belge türlerinin SDP kodları önceden belirlenerek sistemde veya sistem dışında not olarak sık kullanılanlar olarak kaydedilmeli belge üretilirken bu kodlardan faydalanılmalıdır. Bununla beraber kurumsal olarak SDP üzerinde yapılacak en önemli işlem yine birimlerin faaliyetleri sonucunda sıklıkla oluşan belge

şablonları her birime has SDP kodlarıyla eşleştirilerek yüklenmeli ve kullanıcının belge üretirken bu şablonları kullanması sağlanmalıdır. Böylece SDP konusundaki hatalar asgari düzeye çekilebilecektir.

Kamu kurum ve kuruluşlarında karşılaşılan bir diğer durum ise güvenlik ve belgeyi bulamama endişesi sonucunda elektronik ortamda üretilen her belgenin çıktısının alınarak fiziksel ortamda dosyalanmasıdır. Bu hatalı ve gereksiz uygulamaya dosyalama yapamayan bazı birimlerin de başvurduğu görülmüştür.

Kurumsal SDP kodları dışında kuruma ait iş ve işlemleri özel klasörler açarak yönetmek gerekebilir. Bu kodlar, varsa kurumun karar verdiği kısaltmalar ve kodlamalarla beraber köşeli parantez yardımıyla da uygulanabilir ([ ]). Genellikle Hukuk, Teftiş ve Personel birimlerinin başvurduğu bu özel klasörler; ihale dosyaları, personel sicil dosyaları, dava dosyaları ve proje dosyaları gibi sadece bir birim veya bir kişi tarafından görüntülenmesi gereken klasörlerdir. Program, yetkili elektronik belge yöneticisi tarafından kurallı bir şekilde SDP kodlarıyla ilişkili köşeli parantez içerisinde bir kod açılabilmesini ve bu koda bağlı bir klasör oluşturulmasını sağlamalıdır.

Özel kodların istenilen ve standart bir düzende olması için kontrollü terminoloji kullanılması ve kod açma yetkisinin sadece belirli kişilerde olması (Birim Belge Yöneticisi veya Belge Yöneticisi) gerekmektedir. Bunun için öncelikle bu kodlara ihtiyaç duyan birimlerle görüşülerek ortaya çıkan terminoloji ile ilgili olarak (Personel dosyaları için sicil numarası veya T.C. kimlik numarası, dava dosyalarında esas numaraları gibi) belge yöneticisi tarafından özel kodlu klasörler açılabilmelidir. Belge üreticileri de konu koduyla ürettikleri belgeleri özel kod yardımıyla farklı konulara ait belgeleri tek bir klasörde birleştirerek üzerinde çalışacağı iş ve işlemler bakımından dosya bütünlüğünü sağlamış olacaktır.

Kurumsal iş ve işlemleri yürütürken arşivle beraber dosyalama ve dosya bütünlüğü de çok önemlidir. Elektronik ortamda da bu entelektüel bütünlük konu veya vaka bağlamında sistem içerisinde yönetilerek dosyalanmalı, yani klasik arşivcilikte uygulanan metotlar elektronik ortamda uyarlanmış şekliyle karşılık bulmalıdır. Dosyalama işleminin EBYS'de belgeleri tek tek dosyalamak gibi sıradan basit bir işlem olarak algılanması ve SDP'nin tek başına dosyalamada yeterli olacağının düşünülmesi uygulamalarda hataya düşürmektedir. Nitelikli dosyalama ve erişim unsurunun kısıtlanması gibi algılanan bu durumda özel kodlar ve bazı gerekli üst veri alanlarının kurumsal veya birimsel fonksiyonlar çerçevesinde belge üreticilerine sunulması gerekmektedir. Milli hafıza bakımından da çok önemli bir unsur haline gelen bu üst veri alanlarıyla bundan 100 yıl sonrasında hak kayıpları veya bilgi kayıplarının önüne geçilmesi adına tanımlamalar yapılmalıdır. 100 yıl sonrasında bir belgeye erişmek için SDP kodları veya özel tanımlamalar yeterli olmayan durumları karşımıza çıkabilir. Veya içerik aramalarıyla üzerinden uzun zaman geçmiş bir belge nitelikli arama yapılarak karşımıza çıkamayabilir.

Sonuç

Elektronik Belge Yönetim Sistemleri sadece kurumsal fonksiyonları yerine getirirken kullanılan belge üretim ve paylaşım araçları değildir. Kurumların her türlü bilgi ve belgelerinin içerik ve ilişkisel özelliklerinin korunarak üretiminden tasfiye sürecine kadar geçen sürede bütün süreçleriyle yönetilmesini ifade etmektedir. Sistem dinamiklerinin arşivcilik anlayışıyla beraber hareket etmesi gereken bu sistemlerde teknolojik değişkenliklerin ve sistemsel sıkıntıların bilgi ve belgelerin geleceğe aktarımında bir engel teşkil etmemesi de önemli bir husustur.

Devlet Arşivleri Genel Müdürlüğü olarak yapılan denetim faaliyetleri ile tespit edilen sorunlar kamu kurum ve kuruluşları için ileride doğabilecek hukuki sorunlar ve arşivcilik anlamındaki zafiyetlerin önüne geçebilmek adına en yakın zamanda EBYS konusunda gerekli tedbirlerin alınarak mevzuata uygun hareket edilmesi sağlanmalıdır. Klasik arşivcilikteki sorunların elektronik ortama da taşınması kurumlarda belge yönetim ve arşiv süreçleri bakımından sıkıntılı süreçler yaratabilir. Arşivin en önemli hedefi eldeki mevcut materyali gelecek nesillere aktarmak olduğu için elektronik ortamda belgelerin ıslak imzalı belgelere oranla hukuki geçerliliğini, içerik ilişkisini ve form özelliğini kısacası özgünlüğünü koruyarak bu hedefi gerçekleştirmek daha zor bir durumdur. Teknolojik eskimeler sonucunda yenilenen format, yazılım ve donanım değişiklikleriyle eski teknolojilerle üretilen elektronik belgelere erişimin sorunsuz olabilmesi dikkat edilecek hususların başında gelmektedir. Milli hafıza bakımından uzun vadede düşünüldüğünde elektronik materyallerin ilerleyen zamanlarda kullanılamaz duruma gelmesi veya çok yüklü miktarda ödemelerle yeni teknolojilere çok kısa vadedeki güncellemeler veya geçişler kurumların yükünü arttırabilir.

Kamu kurum ve kuruluşlarında üretilen elektronik belgeler ıslak imzalı belgelerde olduğu gibi kamu faaliyetlerini ve bilgilerinin korunması ve hesap verilebilirliğin sağlanması, hak kayıplarının önüne geçilmesi, kamu faaliyetlerinin etkili ve verimli bir şekilde yürütülebilmesi açısından aynı derecede öneme sahiptir.

Kaynakça

Başbakanlık. (2005). 2005/7 sayılı Standart Dosya Planı Genelge. 1 Haziran 2017 tarihinde *http://www.resmigazete.gov.tr/eskiler/2005/03/20050325-10.htm* adresinden erişildi.

Başbakanlık. (2008) 2008/16 sayılı 2008/16 sayılı, Elektronik Belge Standartlarına Dair Genelge. 2 Haziran 2017 tarihinde

http://www.resmigazete.gov.tr/eskiler/2008/07/20080716-7.htm adresinden erişildi.

Başbakanlık. (2015). Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. 5 Haziran 2017 tarihinde *http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/*

2015/02/20150202.htm&main=http://www.resmigazete.gov.tr/eskiler/2015/02/20150202.htm adresinden erişildi.

Devlet Arşivleri Genel Müdürlüğü. (2009). Standart Dosya Planı Açıklamalar ve Kurallar. 7 Haziran 2017 tarihinde

http://www.devletarsivleri.gov.tr/icerik/319/standart-dosya-plani-sdp/ adresinden erişildi.

Türk Standartları Enstitüsü. *TS 13298 (2015)Elektronik Belge Yönetimi Standardı*.

Elektronik İmza Kanunu. (2004). T.C. Resmi Gazete. 25355. 23 Ocak 2014.

Elektronik Arşiv Yönetim Sistemleri ve Kurumsal Etkileri

Electronic Archive Management Systems and Organizational Effects

Hüseyin ÜNAL
Anadolu Ajansı Arşiv Müdürü

Özet

Teknolojinin en hızlı geliştiği ve en fazla kullanıldığı ortamlardan birisi de hiç kuşkusuz bilgiyi konu edinen alanlardır. Bu alandaki gelişmeler ve buna bağlı olarak ortaya çıkan fırsatlar bilgi ile ilgili süreçlerde teknolojinin yoğun bir şekilde kullanılmasını sağlamıştır. Bunun bir sonucu olarak bilginin sistematik bir şekilde üretildiği ve kullanıldığı kurumsallaşmış yapılarda bilginin oluşturulması, iletilmesi ve saklanması ile ilgili süreçler de giderek daha fazla elektronik ortama taşınmaya başlanmıştır. Bilgi, kurumsal yapılarda genellikle ilişkisel ve listelenmiş veri olarak veya belli bir formatta hazırlanmış doküman olarak yönetilir. Bu çalışmada temel olarak, kurumsal yapılarda, belge-doküman formundaki bilginin elektronik ortamda yönetilmesi ile ilgili süreçler ele alınacaktır. Kurumlar, yapıları gereği yerine getirdikleri faaliyetler esnasında bir takım bilgi ve belge üretirler. Üretilen bu bilgi ve belgeler gerçekleştirilen kurumsal faaliyetlerin kanıtı niteliğindedir. Kurumlar hesap verebilir ve hesap sorabilir yapılardır. Bu hesap verme ve hesap sorma süreçleri de genellikle gerçekleştirilen faaliyetlerin kanıtı niteliğinde olan belgeler üzerinden yürütülmektedir. Bu sürecin gerçekleştirilmesi ve sürdürülebilirliği için de üretilen bilgi-belgelerin uzun süre saklanmasını ve ihtiyaç halinde de kolayca erişilebilir olmasını sağlayan sistemlere ihtiyaç duyulmaktadır. Günümüzde bu tür ihtiyaçlar için en uygun ortam elektronik ortamlardır. Bu çalışmada, kurumsal bilgi-belge-dokümanların elektronik olarak uzun dönem arşivlenmesi için gereken hususlar ve yöntemler ortaya konmaya çalışılmıştır. Çalışmada, geleneksel ortamda üretilmiş belge-dokümanların elektronik ortama aktarılması için işletilecek olan süreçler, elektronik arşiv sistemlerinin sahip olması gereken yapısal özellikler, elektronik ortamda üretilmiş belge-dokümanların elektronik arşivlere aktarılması, elektronik arşivlerin diğer sistemler ile bütünleşme gibi konulara açıklık getirmeye çalışılacaktır. Çalışmanın sonunda bir bilgi ve belge sistemi oluştururken göz önünde bulundurulması gereken ilkeler ve önerilere yer verilecektir.

Anahtar kelimeler: *Elektronik Arşiv Yönetimi, Elektronik Arşiv Yönetim Sistemi Uygulama Geliştirme, Kurumsal Bilginin Organizasyonu, Bilgi Güvenliği, Birlikte Çalışabilirlik.*

Summary

One of the fields in which the technology advances fastest and the most used is undoubtedly the field of knowledge the developments on technology and resulting opportunities have

enabled the use of technology in information-related processes intensively. As a result of this, organizations which produced information systematically started to move informational process more and more to electronic format to create, make reachable and preserve. Information is usually managed as relational and listed data or as a document which prepared in a certain format in institutional structures. In this study, related processes of the information which prepared as document form on the electronic environment in institutional structures will be discussed. Institutions produce a number of information and documents during the activities they perform. These produced information and documents are evidence of the institutional activities carried out. Institutions are the structures that can call somebody to account or answer for someone or something. These accountability processes are also carried out on documents which are evidence of the activities carried out. In order for this process to be pursue and to be able to continue for a long period, there is a need for systems that ensure the produced information-documents are stored for a long time and are easily accessible when needed. Today, electronic systems are the most suitable environment for such needs. Management of electronic documents which are being used intensively in institutional structures, originality and integrity are the most fundamental elements that must be protected in the work to be done regarding the electronic document management systems. Providing healthy solutions to guarantee the authenticity and integrity of document is crucial to the success of electronic document management systems or electronic archive systems. In this article, the necessary elements and methods have been put forward for long-term electronic archiving of institutional documents. The main topics that covered in the study are the processes to be carried out in order to transfer the document which produced as traditionally to the electronic environment, what structural characteristics of the electronic archive systems should have, how to transfer the document which produced in the electronic environment to the electronic archives, how to integrate the electronic archives with other systems. At the end of the work, the principles and recommendations will be put while creating an information and documentation system.

Keywords: *Electronic Document-Document Management, Electronic Archive Management System Developing Software, Organization Of Enterprise Information, Information Security, Interoperability.*

Giriş

Çok hızlı gelişen ve değişen teknoloji, kurumlarda iş verimliliğini artırmada başvurulan en önemli unsurlarından biri haline gelmiştir. Teknolojinin en çok kullanıldığı alanlardan birisi de hiç kuşkusuz bilginin yönetilmesiyle ilgili süreçlerdir. Birçok kurum iş süreçlerini ve bu süreçlerde oluşturulması zorunlu bilgi ve belgelerini elektronik ortama taşımaktadır. Bu süreçleri ilk defa elektronik ortama taşıyan kurumların birçok sorunla baş etmeleri gerekmektedir. Kurumların bu bağlamda gereksinim duydukları sistemlerin geliştirilebilmesi için birçok koşulun incelenmesi ve mevcut uygulamalarda yaşadıkları sorunlar ile beklentilerin saptanması gereklidir. Bu sistemlerin en başında da elektronik belge yönetim sistemleri ve elektronik arşivler gelmektedir. Bu sistemler her ne kadar ortak yönlere sahip olsalar da farklı ihtiyaçları karşılamak için oluşturulduklarından dolayı hem işlev hem de yapı olarak birbirlerinden oldukça farklıdırlar.

Elektronik Belge Yönetim Sistemi (EBYS), kurum ve kuruluşların iş ve işlemlerini yerine getirirken yapmış oldukları tüm yazışmaların orijinal özelliklerinin ve içeriklerinin korunarak elektronik ortamda oluşturulması, gönderilmesi, saklanması kısacası bir belgenin geçirdiği tüm evreler boyunca yönetilmesini sağlayan sistemdir (Atilla, Mansur ve Uslu, 2015, s.1; Odabaş, 2009, s.415). Arşivler ise; kurumların, gerçek ve tüzel kişilerin meydana getirdiği hizmetler, haberleşme ve işlemler sonucu oluşan, zaman içerisinde biriken, toplanan ve amacına göre farklı nedenlerle saklanan her türlü materyal ve bu materyallerin saklandığı, korunduğu yerler olarak tanımlanmaktadır (Ayliz, 2013, s.1). Belgelerin kanıt olma özelliğine vurgu yapan Kandur (2006, s.15) elektronik belge yönetim sistemlerinin amacını; kurumların rutin işlerini yerine getirirken oluşturdukları, kurum işlemlerinin kanıtı niteliğinde olan belgelerin, elektronik ortamda içerik, format ve ilişkisel özelliklerini koruyarak, çoklu kullanımına imkân veren yapının oluşturulması olarak açıklamaktadır. Bu sistemle, belgelerin yaşam döngüsü süresince zaman ve mekân sınırlaması olmadan, kolay ve tek noktadan erişilebilir olması sağlanarak bilginin etkin bir şekilde yönetildiği verimli çalışma ortamları oluşturulabilir. Deneyimlerimiz belgelerin elektronik ortamlarda üretiliyor ve yönetiliyor olmasının sağladığı kolaylıklar ile zaman zaman elektronik ortamda olmayan belgelerin de bu sistemlerde kullanılma ihtiyacı, zaten birçok kurum için gündemde olan arşiv belgelerinin de elektronik ortama aktarılmasını gereklilik haline getirdiğini göstermektedir. Bununla birlikte kurumlardaki iş ve iş süreçlerinin neredeyse tamamının elektronik ortamda yürütülüyor olması, arşivlerin de bu kapsama dâhil edilmesini kaçınılmaz kılmaktadır. Bu gereksinimleri göz önünde bulunduran çalışmamızda, bir kurumun bilgi yönetimi bağlamında bir elektronik arşiv yönetim sisteminin oluşturabilmesi için hangi unsurların ele alınması ve nasıl bir yapıya sahip olması gerektiği ile ilgili görüşler ortaya konmaya çalışılacaktır.

Kurumun tüm ihtiyaçlarını karşılayabilecek bir elektronik arşiv yönetim sisteminin başarılı bir şekilde oluşturulabilmesi için, öncelikle kurum yapıları ve kurumda bilgiyi en yoğun kullanan yönetici kesim ile ilgili bazı özelliklerin ortaya konması faydalı olacağı düşünülmektedir.

“Kurum, bir sosyal grup ya da toplumda belli amaçları gerçekleştirmeye yönelik olarak temel işlevleri karşılayan, süreklilik kazanmış, diğer kurumsal yapılarla ilişkili, ancak kendi alanında tek olan ve kendine özgü değerler taşıyan bir sistemdir” (Özdemirci, 1999, s.367). Kurumlar bulundukları çevre içerisinde belli bir fonksiyonu yerine getirmek amacıyla kurulmuşlardır. Kurumlar, varoluş amaçlarını yerine getirmek adına ihtiyaç duyduğu beşeri, ekonomik ve maddi araçlarla donatılması ve sahip olduğu bu araçları verimli ve etkili bir şekilde çalıştırma adına, çeşitli düzenleyici faaliyetlerde bulunur. Bu anlamda düzenleme, kurumun amaçlarına ulaşabilmesi için hangi işlevleri yapması gerektiğine ve bu işlevleri yapacak birimlerin birbirleriyle uyumlu çalışacak şekilde oluşturulmasına, bu birimlerde çalıştırılmak üzere gerekli olan beşeri ve maddi

sermaye unsurlarının tedariki ve uyumlu hale getirilmesine ilişkin süreçlerden oluşmaktadır. Tüm bu süreçlerin gerçekleştirilmesi ise yönetimsel bir faaliyet gerektirir. Yönetim; ortak amaçların etkili ve verimli bir şekilde gerçekleştirilebilmesi için, işbirliği yapmış insan grubunun faaliyetlerinin planlanması, örgütlendirilmesi, yönlendirilmesi, koordinasyonu ve kontrol edilmesiyle ilgili tüm süreçler olarak tanımlanabilir (Dinçer ve Fidan, 1996, s.152; Şahin, 2010, s.25).

Bir kurumun başarısı, üstlendiği işlevi yerine getirerek amaç ve hedeflerine ulaşmasına bağlıdır. Bu da organizasyonlarda etkin bir iletişimi gerektirir. Günümüzde organizasyonların üstlendikleri işlevleri yerine getirerek amaç ve hedeflerine ulaşmaları, yazışmaların yapılmasına, formların kullanılmasına, rapor ve talimatların hazırlanmasına, daha da önemlisi bu kaynakların kullanılmasını da sağlayacak bir sistemin kurumda olmasına bağlıdır (Özdemirci, 2001, s.185).

Kurumlarda organizasyon yapısını, yönetim şeklini ve iletişim biçimlerini etkileyen en önemli unsurların başında bilgi ve teknoloji gelmektedir. Bilgi, iş süreçlerinin her aşamasında kullanılan ve iş süreçlerini etkileyen önemli bir faktör, teknoloji ise bilginin vazgeçilmez bir parçasıdır. Bilgi yönetiminin temel araçları olan kurumsal dinamikler, yönetim modelleri ve teknoloji kurumun bilgiyi elde etmesini, geliştirmesini ve transferini sağlamak üzere bir arada ve uyum içerisinde çalışmalıdır (Odabaş, 2007, s.370).

Kurumun kendine özgü değerler taşıyan bir sistem olması, 'kurumsal bilgi' olgusunu da beraberinde getirmektedir. 'Kurumsal bilgi' kurumların doğuşuyla özgün değerler birikimi olarak ortaya çıkmaktadır (Özdemirci, 2001, s.179). Kurumsal bilgilerin büyük bir kısmını kurumların faaliyetleri esnasında üretilen belgeler oluşturmaktadır. Bu nedenle bu tür belgeler birinci derecede kurumsal bilgi kaynağı olarak görülmektedir. Bu bağlamda kurumsal bilgi, kurumun etkinliği, denetimi, yönetimi, geliştirilmesi ile ilgili olarak üretilen, alınan, kullanılan ve bu nedenlerle özel bir nitelik kazanan her türlü malumat, fikir ve olgulardır (Özdemirci, 2001, s.180). Kalseth ve Cummings (2001, s.167)' e göre ise bilgi yönetimi; kurumlarda her seviyede oluşturulan strateji, politika ve uygulamalara yönelik gerçekleştirilen aktivitelere ilişkin bilgiyi konu alma, entelektüel birikim ile elde edilen başarı arasında neden-sonuç ilişkisi kurmaktır. Kurumsal bilgi yönetiminin amacı, kurumda var olan kayıtlı ve kayıtsız her türlü bilginin ortaya çıkarılması, değerlendirilmesi, organize edilmesi, gereken yerlere ulaştırılması ve kuruma dolaylı bir katma değer kazandırılmasıdır (Odabaş, 2007, s.369).

Kurumda üretilen ve kullanılan bilginin değerini ve amacını belirleyen en önemli unsur, bilginin kurumda gerçekleştirilen faaliyetler esnasında ne derece ve etkinlikte kullanıldığına bağlıdır. Gerçekleştirilen faaliyetlerde kullanılan bilgi; "doğrudan kurumun etkinlikleri ile ilgili olarak gerçekleştirilen eylem ve çalışmaların her aşamasında gereksinim duyulan ve sürekli gelişerek artan işletim

bilgisi ya da bir işin yerine getirilebilmesinden ziyade faaliyetlerin denetimi ve geliştirilmesi için gerekli olan yönetim bilgisi olabilir"(Özdemirci, 2001, s.180).

Bilgi, kurumlarda ürün ve hizmetlere değer katan soyut bir faktördür. Bilgi, kuruma sürdürebilir bir avantaj sağlayan ve kuruluşu yaşatan bir değer olarak karşımıza çıkar. Kurumların bilgiyi yönetme becerileri, rekabet içinde oldukları diğer kurum ve kuruluşlar arasındaki pozisyonunda da belirleyici rol oynamaktadır. Başarılı bir bilgi yönetiminin temel unsurlarından birisi de önemli bilgilerin saptanması, kaydedilmesi ve düzenlenmesi için gerekli sistemin tasarlanması, kurulması ve sistemi destekleyen alt birimlerin oluşturulmasına dayanan yetkinliktir (St. Clair, 2003, s.1486).

Kurumsal bilgi yönetimi temel seviyede ve sistematik olarak ilk önce kurumla beraber aynı anda ortaya çıkan ve kurumun tüm hafızasını derleyen arşivde başlar. Kurumda gerçekleştirilen faaliyetlerin değerlendirilmesi, aynı zamanda yönetimin etkinliğinin de değerlendirilmesi anlamına gelir. Bu değerlendirmeler genellikle kurumda üretilen belgeler üzerinden gerçekleştirildiği için kurumsal bilgi ve belge yönetiminin önemini ortaya çıkmaktadır. Bu durum, kurum ve kuruluşların ürünleri olan belgelerin yönetimi için bir sistem kurma zorunluluğunu da beraberinde getirmektedir. Kurumun en eski bilgi kaynaklarına ev sahipliği yapan arşivlerin, bu tür sistemler içinde yer almaması büyük bir eksiklik doğuracaktır.

Günümüzde kurumsal yapılardaki iş süreçlerinde çok büyük etkisi olan teknoloji, kurum içi ve dışı bilgi iletişiminde de belirleyici unsur olarak karşımıza çıkmaktadır. Bilginin çok zahmetsizce üretilebildiği, dağıtılabildiği ve saklanabildiği elektronik sistemlerin kullanılması kurumlar açısından kaçınılmaz bir durumdur. Bu duruma ayak uydurması gereken arşivler de, ellerinde bulunan bilgi ve belgeleri diğer elektronik sistemlerle uyum içerisinde çalışabilecek bir yapıya dönüştürmek zorundadırlar. Aksi halde, elektronik ortamlarda bilgi kullanmaya alışmış ve kanıksamış bireylere hala geleneksel yapıda hizmet vermeye devam etmek, arşiv birimleri için varlık-gereksinim sorununun doğmasına neden olabilir.

Kurumların hafızası niteliğinde olan arşivler, varlıklarını garanti altına almak ve sürdürmek için, hizmetlerini yeni ihtiyaçlar doğrultusunda yeniden değerlendirmek zorundadır. Teknoloji bu değişimin ve dönüşümün yönünü belirleyecek olan en önemli unsurdur. Özellikle bilgi teknolojilerindeki baş döndürücü gelişmelerin sunduğu fırsatlar ve kolaylıklar, arşiv hizmetlerinin yeniden tasarlanmasında anahtar rol üstlenmektedir. Arşivlerin kendilerini dönüştürmek adına yaptıkları ilk iş, genelde sahip oldukları kaynaklarını elektronik ortama aktarmaktır. Kaynakların elektronik ortama aktarılması değişen çağa uyum sağlamak adına gerçekleştirilmesi zorunlu bir adım olabilir, ancak asla tek başına yeterli değildir. Elektronik ortama aktarılan bilgilerin yönetilmesi için bir uygulamaya ihtiyaç vardır. Bu uygulama arşiv ile kullanıcılar arasında sanal bir köprü görevi görecek ve fiziksel arşivin yerini alacak olan elektronik arşiv yönetim sistemidir.

Kurumda gerçekleştirilecek olan bir elektronik arşiv yönetim sistemi projesi, kurum yapısı, kullanıcı ihtiyaçları ve bilgi kaynaklarının niteliklerinin ortaya konduğu bir *analiz* ile başlar. Analiz sürecinde öncelikle yapılması gerekenleri şöyle sıralayabiliriz;

- Kurumsal bilgi sistemlerinin işleyişini etkileyen ya da belirleyen idari yapı, sosyal ve kültürel çevre ile yasal koşulların analizi,
- Kurumlarda bilgi ya da belge işlemlerinden sorumlu personelin niteliğinin değerlendirilmesi,
- Bilgi ve belge içeriğinin üretildiği birimler ile merkezi idari yapılar arasındaki ilişki ve iletişimin tanımlanması,
- Bilgi içeriğinin üretimi, düzenlenmesi ve dosyalanması, saklama koşullarının tanımlanması, korunması ve güvenliği ile kayba uğramadan uzun süre saklanmasına dönük koşulların ve beklentileri analizi (Külcü ve Çakmak, 2009, s.287).

Analiz aşamasından sonra kapsam belirlenmelidir. Elektronik arşiv sistemi oluşturulurken hangi tür bilgi kaynaklarının kapsama dâhil edileceğine önceden karar verilmesi ve bu konuda mümkünse yazılı bir kıstaslar listesi oluşturması kurulacak olan sistemin ileride yönetilemeyen bir bilgi yığını olmasının önüne geçecektir. Bu doğrultuda kapsam içerisine alınacak bilgi kaynaklarının belirlenmesi esnasında dikkat edilmesi gereken unsurlara ilişkin önerilerimiz şunlardır;

- Bilgi kaynağının niteliği,
- Kurum açısından önemi,
- Miktarı,
- Çalışanların bilgi gereksinimleri,
- Arşiv personelinin sayısı ve yetenekleri,
- Sistem ve donanım altyapısı,
- Maliyeti (Aktarım-tanımlama ve depolama açısından)

Analizi yapılan ve kapsamı belirlenen elektronik arşiv yönetim sisteminde bir sonraki aşama *tasarımdır.* Oluşturulacak olan elektronik arşiv sisteminde yer alacak bilgi kaynaklarının ne şekilde organize edileceği, birbirleriyle ilişkilerinin ne şekilde kurulacağı, dosya sisteminin ne şekilde tutulacağı, kurumdaki diğer sistemler ile birlikte çalışabilirliğinin nasıl sağlanacağı sistem henüz tasarım aşamasındayken karar verilmesi gereken konulardır. Tasarım aşamasında, sistemi etkileyecek, kurumun organizasyon yapısı, iş süreçleri, sistem ve ağ altyapısı, personel sayısı ve nitelikleri, kullanılan diğer bilgi sistemleri, idari ve yasal konular kapsamlı bir şekilde yeniden ele alınmalıdır. Bu sürecin tek bir kişi veya birim tarafından sağlıklı bir şekilde yapılması mümkün olamayacağından, farklı birimlerdeki uzmanlardan oluşturulacak olan bir ekip ile gerçekleştirilmesi projenin başarısı açısından önemlidir.

Bu çalışmalar sonrasında, ortaya konan sistem tasarımı çerçevesinde uygulama geliştirme süreci başlatılabilir. Uygulama geliştirme süreciyle birlikte elektronik

arşiv yönetim sisteminde yer alacak tüm bilgi kaynaklarını kapsayacak şekilde bir dosya planı hazırlanmalıdır. Hali hazırda kullanılan bir dosya planı var ise proje ile kapsama dâhil edilecek olan kaynaklar da göz önünde bulundurularak yeniden değerlendirilmeli varsa eksikler giderilerek sisteme entegre edilmelidir. Bilgi kaynaklarının dosya planına göre sınıflandırılması uzmanlık gerektiren bir konudur. Hayata geçirilecek olan sistemin bu süreci kolaylaştırıcı ve hataları önleyici çözümler sunması yerinde olacaktır.

Elektronik arşiv sisteminin başarısı büyük ölçüde bilgi kaynaklarının tanımlama bilgisiyle ilişkilidir. Bu nedenle bilgi kaynaklarının tanımlama alanlarının belirlenmesine ilişkin analiz çalışmalarında, elde edilen konuyla ilgili bulgular bu süreçte yeniden değerlendirilmelidir. Belirlenecek olan tanımlama bilgileri ne süreci uzatacak kadar ayrıntılı ne de bilginin erişilmesini imkânsız kılacak kadar da yüzeysel olmamalıdır. Tanımlama alanları belirlenirken, bu alanda kullanılabilecek teknolojilerin sunduğu fırsatlar da göz önünde bulundurulmalıdır.

Elektronik arşiv yönetim sistemi için geliştirilen bir uygulamanın bazı temel fonksiyonlara sahip olması beklenir. Bunların başında, uygulama üzerinden gerçekleştirilecek olan işlemlerin belli bir sırayla gerçekleştirilmesini sağlayacak basit düzeyde bir *süreç yönetimi*dir. Süreç yönetimi, bilgi kaynaklarının sisteme girişi, kalite kontrolü, nitelenmesi ve erişimi ile ilgili tüm işlemleri kapsayan sistematik iş akışı şeklinde olabilir. Ayrıca bu sayede süreçlerde yapılması gereken iş miktarı bilgisi de anlık olarak elde edilebilir. Böylece sistemde yavaş giden, aksayan işler tespit edilerek personelin performansları ölçülür ve iş gücünün daha verimli kullanılabilmesi için gerekli önlemler alınabilir. Bir süreç yönetiminin olması, sisteme hatalı bilgi girişini engelleyecek, işlerin daha hızlı ve doğru yapılmasını sağlayacak imkânlar da sunabilir.

Elektronik arşivlerin oluşabilmesi için bilgi kaynaklarına ihtiyaç vardır. Elektronik arşivlerin temel kaynağı genellikle sonradan dijitalleştirilen analog ortamdaki bilgi ve belgelerdir. Dijitalleştirme sürecinin doğru bir şekilde yapılması daha sonradan gerçekleştirilecek olan kalite kontrol, sınıflama ve tanımlama ile ilgili işlerin kolay, hızlı ve daha doğru yapılmasına olumlu katkı sağlayacaktır.

Arşiv materyalleri sahip oldukları özellikler bakımından farklılıklar gösterir. Bu tür farklılıklar dijitalleştirme esnasında mutlaka göz önünde bulundurulmalıdır. Her bir materyal türü için uygun dijitalleştirme cihaz ve yöntemleri kullanılmalı, dijitalleştirme esnasında orijinal materyallerin zarar görmesine neden olabilecek yöntem ve cihazlardan uzak durulmalıdır. Dijitalleştirme sonrasında elde edilen elektronik kopyanın mümkün olduğu kadar orijinal kaynağa en yakın kopya olmasına dikkat edilmelidir.

Standartlaşmış iş ve ürünler için otomasyona geçiş daha kolay ve başarılı bir şekilde gerçekleştirilebilmektedir. Bu nedenle işlerin daha sonradan otomasyona

geçirilebileceği hesaba katılarak, dijitalleştirme esnasında yapılacak işler için kıstaslar belirlenirken elde edilecek çıktının belli bir standartta olması gerektiği göz önünde bulundurulmalıdır.

Elektronik arşiv yönetim sistemine aktarılan bilginin doğruluğu, bütünlüğü ve geçerliliği sistemin başarısı açısından önemlidir. Bu nedenle elektronik arşivdeki her bir bilgi kaynağının son kullanıcıya sunulmadan önce tüm kontrollerinin yapılmış olması gerekir. Yukarıda bahsedilen ve elektronik arşiv yönetim sisteminin sahip olması gereken basit bir süreç yönetiminin bu tür kontroller için de kullanılması uygun olacaktır. Son kullanıcıya sunulacak hatalı bir bilgi tüm sistemin sorgulanmasına neden olabilir ve sisteme duyulan güven zedelenebilir.

Elektronik arşiv sistemleri için son kullanıcıya sunulmadan önce bir bilgi kaynağı en az iki ayrı aşamadan geçmesi, sistemin sağlıklı işlemesi açısından önemli ve gereklidir. Bunlardan birincisi dijitalleştirilen materyallerin teknik ve görsel olarak istenen kıstasları karşılayıp karşılamadığının kontrolü ikincisi ise bilgiye erişimde kullanılacak olan tanımlama bilgilerinin oluşturulmasıdır. Birinci aşamada dijitalleştirilen içeriğin asgari **Tablo-1'**deki kıstaslar çerçevesinde kalite kontrolünün yapılması önerilir;

Tablo-1 Elektronik kopya kalite kontrol kıstasları

Belge / Fotoğraf	**Video/Ses**
Çözünürlük	Çözünürlük
Renk derinliği	Renk derinliği
Dosya Formatı	Dosya formatı (Encode format görüntü için DPX, ses için LPCM)
Sıkıştırma	Sıkıştırma
Netlik	Saniye başına çerçeve sayısı (FPS)
Bütünlük	Ses dosyası için bit derinliği (Kbps) ve frekans aralığı (KHz)
Kesilme-Yırtılma-Katlanma	Ses dosyası için stero-mono
Orijinalinden büyük kopya	
Orijinalinden küçük kopya	
Eğrilik	
Gereksiz veri (siyah çerçeve-nokta)	
Aşırı koyu	
Aşırı Açık	
Üst üste çakışmış tarama	
Elektronik kopya üzerinde çizik	

İkinci aşama olan tanımlama bilgilerinin oluşturulması, elektronik arşiv yönetim sistemlerinde bilginin erişilebilir ve kullanılabilir olmasını sağlayan en önemli aşamadır. Tanımlaması yapılmayan bir materyal elektronik arşiv sistemlerinde erişilebilir olmayacağı için yok hükmündedir. Tanımlama işi zahmetli ve uzun

zaman gerektiren bir süreç olduğu için iyi tasarlanması gerekir. Bu işleminin kalite kontrol işleminden sonra yapılması, yeterli kıstasları taşımayan elektronik kopyaların tanımlamalarının yapılmasının önüne geçerek iş gücünden ve zamandan tasarruf edilmesi sağlanabilir.

Tanımlama için kullanılacak alanların en uygun seviyede belirlenerek hem bu süreç için gereken iş gücü ve zamanın doğru kullanılmasını hem de daha sonradan materyale erişimi mümkün kılması sağlanmalıdır. Bilgi kaynaklarının tanımlama alanlarının belirlenmesi işi, arşiv personeli öncülüğünde bu kaynakları üreten ve kullanacak olan kişilerden oluşturulan bir ekip tarafından ortaklaşa belirlenmesi daha doğru karar alınmasını sağlayacağı düşünülmektedir. Tanımlama alanlarının belirlenmesinde aşağıdaki kıstasların göz önünde bulundurulması beklenir;

- Materyal türü
- Bilgi kaynağı içerisinde barındırdığı bilginin türü,
- Kullanıcıların kaynağı ne şekilde kullandıkları,
- Kullanıcı profili (kişilik, meslek, eğitim açısından)
- Arşiv iş gücü ve uzman personel sayısı,
- Alanda kullanılabilecek teknoloji.

Tanımlama bilgilerinin girilmesi için belirlenen personel mutlaka önceden bilgilendirilmeli ve dikkat edilecek hususlar konusunda uyarılmalıdır. Ayrıca tanımlama bilgilerinin girildiği sistem de hataların oluşmasını engelleyecek önlemler sunmalıdır. Tanımlama alanlarına girilecek verilerin türleri (tarih, sayı, metin vs.) belirlenmeli türe uygun olmayan bilgi girişine müsaade edilmemelidir. Bunlara ek olarak tanımlama alanına girilecek ifadeler için kullanılacak dil de de bir mutabakat sağlanması daha sonradan yapılacak olan aramaların başarısını da olumlu yönde etkileyecektir. Girilen tanımlama bilgilerinin daha sonradan kontrol edilmesinin çok maliyetli olduğu göz önünde bulundurularak bu süreçte görev alacak personelin iyi seçilmiş, iyi bilgilendirilmiş ve eğitim almış olmaları sağlanmalıdır. Girilen bilgiler eğer bir kontrol işlemine tabi tutulacak ise bunun örneklem yoluyla yapılması, hataların yoğunlaştığı yerler var ise bu noktalara özel ikinci bir kontrol uygulanmasının yapılmasının yerinde olacağı düşünülmektedir.

Elektronik arşivlerde yönetilecek bilginin tanımlanması sürecinde var olan teknoloji sonuna kadar kullanılmalı mümkünse geleceğe dönük geliştirilebilecek uygulamalar için de hazırlık yapılmalıdır. Mesela günümüz teknolojisi ile büyük başarı sağlanan optik karakter tanıma (OCR) işlemleri bilgilerin tanımlanmasında ikincil araçlar olarak kullanılabilir. Bununla birlikte ileride çok başarılı bir şekilde gerçekleştirilmesi muhtemel ses tanıma, yüz tanıma ve nesne tanıma gibi araçlar da elektronik arşiv sistemlerine entegre edilerek tanımlama bilgilerinin oluşturulması tamamen otomatik hale getirilebilir.

Tanımlama bilgilerinin oluşturulduğu elektronik arşiv sistemleri içerisinde tanımlama alanları dinamik olarak oluşturulabilmelidir. Oluşturulan bu alanlar

belge gruplarına ve türlerine göre de özelleştirilebilir olmalıdır. Tanımlama sürecinde görevli personelin tanımlama bilgilerinin hatalı girilmesini önlemek adına tanımlama alanına girilecek verilerin zorunlu alan olup olmadıkları, hangi tür verilerin (tarih, metin sayı vs.) girilebileceği gibi sınırlamaların da yine uygulama tarafından belirlenmesine imkân verilmelidir.

Tanımlama bilgilerinin girilmesinden sonra bilgi kaynakları son kullanıcıya erişime açılabilir hale gelmektedir. Ancak bu aşamada dikkat edilmesi gereken en önemli husus hangi bilgiye kimlerin erişebileceği hususudur. Elektronik arşiv yönetim sistemleri geleneksel yöntemlere göre daha fazla güvenlik ve kontrol sunan sistemlerdir. İyi kurgulanmış ve uygulanmış bir sitemle bilgiye yetkisiz erişim neredeyse imkânsız hale getirilebilmektedir. Bilgiye erişim konusunun bilgi güvenliği kapsamında değerlendirilerek ele alınmalı ve konu daha geniş bir çerçeveden değerlendirilmelidir.

Bilgi güvenliği, kurumların sürekliliğinin sağlanmasında büyük önem taşır ve kurumun başta elektronik olmak üzere, çeşitli ortamlardaki kritik bilgilerinin ve diğer bilgi varlıklarının korunması için ele alınması gereken konuları ele alır. Elektronik arşivlerde yönetilen bilginin güvenliği, üzerinde ayrıca durulması gereken önemli konulardan birisidir. Fiziksel arşiv ortamlarına göre nispeten daha güvenli ve kontrol edilebilir ortam sunan elektronik arşivlerde, bilgi güvenliği konusu gereği gibi ele alınmadığı takdirde büyük problemlere neden olabilir. Bilgi güvenliği, bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasının yanı sıra açıklana bilirlik, inkâr edememe ve güvenilirlik gibi diğer özelliklerini de kapsayan geniş bir kavramdır (TS ISO/IEC 27001, 2006). Kurumlarda "bilmesi gerektiği kadar, en az yetki, erişmesi gerektiği kadar" gibi ilkelere en öncelikli uyması gereken gruplar yöneticiler ve bilişimcilerdir. Oysa tam tersine bu ilkelerin en az uygulandığı ve en riskli eylemlerin yaşandığı (zorunlu veya keyfi, bilinçli veya bilinçsiz) birimler de yine bu iki gruptaki çalışanlardır. Kurumlarda en değerli ve en gizli bilgileri kullanan, taşıyan, kaydedenlerin çoğunlukla bu iki gruptaki çalışanlar olduğu bilinmektedir. Ayrıca, işlerinin niteliği gereği kurum genelinde en sık örnek alınan ve daha çok dikkat çeken birimler de gene bu iki birimdir (Tipton ve Krause, 2007, s.873). Elektronik arşiv yönetim sistemlerinde bilgi güvenliği yazılımı, sistemi ve insan boyutlarının tümünün birlikte ele alınması ve değerlendirilmesi gereken bir konu olarak karşımıza çıkmaktadır.

Konunun yazılım boyutu arşivdeki bilgilerin ne tür bir yapıda tutulacağını ve bunlar arasındaki ilişkilerin ne şekilde sağlanacağı ile ilgilidir. Bir elektronik arşiv yönetim sisteminde dosyalar ya 'dizin yapısında' ya da 'binary modda veri tabanında' tutulmaktadır. Dosyaların dizin yapısında tutulması, sunucu üzerinde yetkisi olan kişilerin dosyalara her türlü erişebileceği isterse değiştirebileceği ve bunun da kaydının tutulmadığı durumlarda, güvenlik açısından büyük riskler oluşabileceği unutulmamalıdır.

Dosyaların diskte depolanması için iki farklı depolama teknolojisi kullanılır (Kahveci ve Yenen, 2014, s.78):

1- **SAN (Storage Area Networks)** Depolama Alanı Ağları, depolama kaynaklarındaki verilere sürekli, daha hızlı, daha kolay erişim sağlamak için kullanılan bir teknolojidir. Paylaşılmış depolama birimlerinin bulunduğu yüksek hızlı ağdır. Lokal sunucu (LAN - Yerel ağ) veya uzak bir sunucu (WAN - Geniş alan ağı) üzerindeki bütün depolama cihazları, SAN teknolojisi ile bütün ağ tarafından kullanılabilir durumda olur. Daha fazla depolama cihazı ağa eklenerek, ağdaki depolama yapacak birimlerin hizmetine sunulabilir.

2- **NAS (Network Attached Storage)**Ağa Bağlı Depolama, ağ üzerindeki cihazlar tarafından erişilebilen, gönderilen veriyi depolayan ve bu veriye erişimi sağlayan, içerisinde gömülü bir işletim sistemi bulunan ve klasik sunucu sistemlerindeki client/server ilişkisini esas alan bir sistemdir. Gereksinimlere göre, NAS cihazlarının kapasitesi ek diskler ile genişletilebilir. Dosya sunucusu (file server) yerine NAS cihazlarının kullanılmasının nedeni güvenliktir. Dosya sunucularında olduğu gibi, NAS cihazlarında işletim sisteminin istemci tarafı olmadığı için gelen saldırılara karşı daha güvenlidir. Bu sunucular bazı dosya iletişim protokollerinin bir veya bir kaç tanesini bir arada bulundurabilirler.

SAN sistemler daha fazla yönetilebilirlik seçeneği sağlarken **NAS** sistemler harici hard diskler kadar basit olabilmektedir. Hangi sistem kullanılırsa kullanılsın veri güvenliği açısından kullanılacak sistemin izleme (auditing) yeteneğinin olup olmadığı mutlaka göz önünde bulundurulmalıdır. Dosyalara elektronik arşiv yönetim sistemi harici erişimler de izlenmek isteniyorsa bu yetenek mutlaka sağlanmalıdır. **SAN** veya **NAS** depolama cihazlarına izleme aktif değilken yapılan erişimler herhangi bir şekilde tespit edilemeyeceği için, arşiv dosyalarının dosya sisteminde tutulması durumunda, dosyaların erişilemez olması isteniyorsa mutlaka dosya bazlı kriptolama yöntemlerinden biri kullanılmalıdır. Ancak kriptolama işleminin sistemde çok ciddi yavaşlamaya neden olacağı da göz önünde bulundurulmalıdır. Bu tür risklerin ortadan kaldırılması veya en azından yapılan işlemlerin çok daha rahat denetlenebildiği veri tabanı yapısında dosyaların tutulması daha güvenli olduğu düşünülmektedir. Geneli ilgilendiren, açığa çıkması durumda kişisel kurumsal zarar doğurmayacak belge türleri için “dizin yapısı”, açığa çıkması veya yetkisiz erişim olması durumunda kişisel veya kurumsal zarara neden olabilecek belge türleri için ise saklama alanı olarak ilişkisel veri tabanı servisleri tercih edilebilir. Bunlara ek olarak güvenliği daha ön plana çıkaran “dosya bazlı veri tabanı” da tercih edilebilir. Dosya bazlı veri tabanları bağımsız veri tabanları olup kurulum ve sistemsel bir yönetim gerektirmediği için daha güvenli bir yapı sunabilmektedir. Hangi kayıt ortamı kullanılırsa kullanılsın kriptolama seçeneğinin mümkün olduğu ve fakat aynı zamanda ciddi maliyet getireceği dikkate alınmalıdır. Arşiv uygulamaları için tercih edilebilecek elektronik dosya saklama sistemleri genel olarak Tablo-2’de değerlendirilmiştir. Tablo-2’nin oluşturulmasında güvenlik ve performans unsurları dikkate alınmıştır.

Tablo-2 Elektronik dosya saklama sistemlerinin karşılaştırılması

Sistemler	Olumlu Yönleri	Olumsuz Yönleri
Dosya Sistemi	- Büyük dosyalara erişim çok hızlı - Arşive toplu dosya eklemek veya toplu silmek çok kolay - Arşivin büyükçe bir bölümünün dışarıya kopyasının çıkarılması kolaydır	- Küçük dosyalara erişim çok yavaş - Veri güvenliği zayıftır - Sadece değişen içeriğin yedeklenmesi zor
İlişkisel Veri tabanı	- Veri güvenliği yüksektir - Her türlü yedeklenmesi kolay - Küçük dosyalara erişim çok hızlı	- Büyük dosyalara erişim yavaş - Arşive toplu dosya eklemek için arşiv yazılımı ara yüzü kullanılmalı - Arşivin büyükçe bir bölümünün dışarıya kopyasının çıkarılması zordur
Dosya Veri tabanı	- Büyük dosyalara erişim hızlı - Küçük dosyalara erişim çok hızlı - Veri güvenliği yüksektir - Her türlü yedeklenmesi kolay	- Arşive toplu dosya eklemek için arşiv yazılımı ara yüzü kullanılmalı - Arşivin büyükçe bir bölümünün dışarıya kopyasının çıkarılması zordur

Elektronik ortamda yürütülen tüm işlemlerin; sunucular, istemciler, depolama üniteleri ve ağlardan oluşan belli bir sistem mimarisi içerisinde gerçekleştirilmek zorunda olduğu bilinen bir gerçektir. Tüm bu bileşenlerin birbirleriyle uyumlu ve doğru bir şekilde çalışabilmesi için sistemin iyi kurgulanmış bir mimariye (topoloji) sahip olmaları gerekmektedir. Kurumsal yapılarda elektronik sistemlerin yönetimi genel olarak ayrı bir birim ve uzman kişiler tarafından gerçekleştirildiği gözlemlenmektedir. Dolayısıyla belli bir aşamadan sonra bilgi güvenliği ile ilgili konular bilginin üretildiği, saklandığı, yönetildiği birimlerin dışında başka bir birimin de sorumluluğu altına girebilmektedir. Burada kurum yönetimin, bilgi güvenliği meselesini mümkün olan en üst boyutuyla ele alıp tüm bileşenleri kapsayacak şekilde değerlendirmesinin güvenlik riskini en aza indireceği düşünülmektedir.

Mitnick ve Simon (2011, s.287) da yukarıda anlatılan güvenlik ile ilgili düşüncelerimizi destekler biçimde; kurumlardaki üst yönetimlerin, bilgi güvenliğini bilişim personelinin çözmesi gereken teknik bir iş ve basit bir yatırım gibi gördüğü sürece sorunlar ve risklerin azalmadığını, tam tersine katlanarak arttığını ifade etmektedir.

Bilgi güvenliği yönetiminde, insan ve sürecin hemen her aşamada teknolojiyle birlikte düşünülmesi gerektiği unutulmamalıdır. Her ne kadar teknoloji sayesinde birçok güvenlik sorunu çözülse de insan faktörünün bir şekilde işin içinde olduğu sistemlerde bu faktörün göz ardı edilmemesi gerekir. Konunun insan boyutunu dikkate almadan yapılan çalışmaların eksik kalacağı göz önünde bulundurulmalıdır. Bilinmelidir ki nerede, ne zaman ve nasıl davranacağı kesin bir doğrulukla bilinemeyen ve kontrol altına alınamayan insan faktörü, günümüzde sistemlerin en zayıf halkalarını oluşturmaktadır. Bu nedenle bilgi güvenliğinin sağlanmasında risklere ve tehlikelere karşı kullanıcıların veya personelin mutlaka bilgilendirilerek eğitilmesi gerekmektedir. Bilgi güvenliği, başlanıp bitirilecek bir çalışma, bir iş değildir. Bilgi güvenliği yönetimi, kurumlar ve bilgiler var olduğu sürece sürekli yönetilmesi, denetlenmesi gereken bir yaşam döngüsüdür (Eminağaoğlu ve Gökşen, 2009, s.9).

Elektronik arşiv yönetim sistemlerinde 'güvenlik' konusu, 'bilgiye erişimde yetkilendirme' boyutuyla değerlendirilmesi gereken bir konu olduğu düşünülmektedir. Yukarıda da bahsedildiği gibi güvenliğin diğer boyutları kurumdaki başka birimlerin sorumluluğu ve yetkisi altındadır. Yetkilendirme; bilginin yetkisi olmayan kişilerce erişilemez hale getirilmesini sağlamaya yönelik uygulamaları kapsar. Yetkilendirmenin en önemli unsuru da şüphesiz kimlik tespitidir. Bilgi güvenliği kapsamında kimlik tespiti; "bilgi sistemlerinden hizmet alan alıcının, iddia ettiği kişi olduğundan emin olunması" olarak kullanılmaktadır (Marcinkowski ve Stanton, 2003, s.2528). Kanımızca yetkilendirme sürecinde aşağıdaki adımların sırasıyla uygulanması yetki yönetiminin kolay ve güvenli bir şekilde yapılmasına olanak sağlayacaktır.

- Organizasyon şeması ve kullanıcı pozisyonlarının netleştirilmelidir.
- Yetki dağıtımı (delegasyon) sağlanmalıdır.
- Kullanıcı grupları oluşturulmalıdır.
- Yetkiler belirlenmeli ve kullanıcı gruplarıyla ilişkilendirilmelidir.
- Kişiler, kullanıcı gruplarına atanmalıdır.
- Kullanıcılara ayrıcalıklar (gizli belgelere erişim gibi) tanımlanabilmelidir.
- Tüm iş, görev ve yetki tanımlamaları veri tabanında güncellenebilir, esnek ve erişilebilir bir yapıda tutulmalıdır.

Kendi bünyesinde doğruluk, bütünlük, güvenlik, erişilebilirlik gibi konularda yetkinliği sağlanmış elektronik arşiv yönetim sistemlerinin etkinliğinin artırılması adına, kurumdaki diğer sistemlerle birlikte çalışabilirliğinin de sağlanmasının verimliliğe olumlu katkısı olacağı düşünülmektedir. Özellikle bilgi temelli sistemlerde yaşanan hızlı gelişme, sistemlerin birbirleriyle çok kolay bir şekilde "birlikte çalışmasına" imkân tanımıştır. "Bir sistemin ya da sürecin, ortak standartlar çerçevesinde bir diğer sistemin ya da sürecin bilgisini ve/veya

işlevlerini kullanabilme yeteneği" (Kalkınma Bakanlığı, 2012, s.4) olarak tanımlanan "birlikte çalışabilirlik", verimliliği önemseyen kurumlar için olmazsa olmaz ilkelerden birisi haline gelmiştir. Birlikte çalışabilirlik farklı uygulamalar arasında bilgi paylaşımını merkeze alan teknik boyut, süreç modelleme dilleri ve nesneye dayalı (objectoriented) yazılım geliştirme mühendislik metodolojisini konu edinen organizasyonel boyut ve verinin üretildiği sistem dışındaki sistemler tarafından doğru anlaşılabilmesi ve yorumlanmasına yönelik çalışmaları içeren anlamsal boyut olarak üç boyutta değerlendirilebilir (Kalkınma Bakanlığı, 2012, ss.5-6). Birlikte çalışan sistemler üzerinde gerçekleştirilen işlemler sayesinde bir sistemden elde edilen çıktı anında ve otomatik olarak bir başka sistemin girdisi haline gelerek işlemlerin çok hızlı ve doğru bir şekilde gerçekleştirilmesine olanak sağlamaktadır. Tüm boyutlarıyla ilgili diğer sistemlerle birlikte çalışan bir arşiv yönetim sisteminin etkinliği ve önemi, tek başına çalışan bir sistemden çok daha fazla olacağı değerlendirilmektedir.

Sonuç ve Değerlendirme

Kanımızca bilgi sistemleri, kurumların işleyişi ve iş süreçleriyle ilgili konularda, önemli bir etken hatta kimi durumlarda belirleyici bir unsurdur. Kurumda, farklı birçok bilgiyi yöneten sistemler olsa da en doğru bilgi kaynağı sayılabilecek olan arşivlerin, bilgi yönetim sistemlerinin en önemli bileşenlerinden birisi olduğu yadsınamaz bir gerçektir. Kurumlar açısından bilginin bu kadar önemli bir değer haline geldiği günümüzde arşivlerin de önemi giderek artmaktadır. Geleneksel yöntemlerle idare edilen bir arşivin kurumun güncel ihtiyaçlarına cevap vermesi pek mümkün görünmemektedir. Bu nedenle elektronik bilgi sistemlerinin bir parçası haline gelen arşivlerin ve verdikleri hizmetlerin günümüz koşullarına uygun ihtiyaçlara cevap verebilmesi için yapılması gerekenler genel olarak aşağıda açıklanmaya çalışılmıştır;

- Değişim sürecinde arşivlerin, faaliyet gösterdikleri kurumların tüm içeriğini yönetmeye yönelik kapsayıcı esnek ve birlikte çalışabilirlik prensiplerini esas alan yenilikçi politikalar üretmeye yönlendirmesi gerekmektedir.
- Kurum, sahip olduğu bilginin yönetilmesi için geliştirmiş olduğu politikalar politikalara uygun uygulamaları hayata geçirerek işin sürekliliğini sağlamalıdır.
- Geleneksel olarak oluşturulmuş arşivlerin fiziksel düzenlemelerinin standartlara uygun olarak yapılmış olması gerekmektedir.
- Kurumun tüm bilgi kaynaklarını kapsayacak şekilde özelleştirilmiş bir standart dosya planını olmalıdır.

- Kurum, bilgi kaynaklarının yönetilmesi için elektronik ortamların getirdiği fayda ve fırsatları göz önünde bulundurarak bilgi kaynaklarının elektronik ortama taşınması, elektronik ortamda oluşturulması, yönetilmesi, saklanması ve erişilmesi ile ilgili idari, yasal ve teknik altyapıyı hazır hale getirmelidir.
- Kurumda oluşturulacak olan bilgi sistemlerinin birlikte çalışabilirliği temel ilke olarak benimsenmeli ve geliştirilecek olan tüm uygulamalar için birlikte çalışabilirlik esas alınmalıdır.
- Bilgi güvenliği sürekli gündemde tutulmalı değişen koşullar çerçevesinde yeniden ele alınarak oluşan ve oluşabilecek zaaflara karşı tedbirlerin önceden alınmasını sağlayacak yöntemler geliştirilmelidir.
- Analog ortamlarda oluşturulan bilgilerin elektronik ortama aktarılması veya elektronik bilgi sistemleriyle bir şekilde bağının kurularak izlenmesi ve erişilmesi sağlanmalıdır.
- Elektronik bilgi sistemleri, yönettiği bilgilerin, doğruluğu, bütünlüğü ve geçerliliğinin korunduğu ve ihtiyaç halinde bunların doğrulanabildiği bir yapıda tasarlanmalıdır.
- Elektronik bilgi sistemleri kullanıcıların ihtiyaçlarına hızlı, doğru ve zahmetsiz bir şekilde cevap vermeli, iş gücünün verimli kullanılmasına katkı sağlamalıdır.
- Elektronik bilgi hizmetlerinin tasarlanması, yürütülmesi ve sürdürülebilirliği konularında görevlendirilecek personelin, konuyla ilgili bilgi sahibi olması ve gerekli eğitimlerin verilerek sürekli güncel kalması sağlanmalıdır.
- Arşivcilik açısından yeni bir döneme girdiğimiz bu günlerde, arşiv çalışanlarının da bu yeni dönemin gereksinimlerini analiz edebilecek, çözüm önerileri sunabilecek ve bunları hayata geçirebilecek donanıma sahip olmaları gerekmektedir.

Kurumların bilgi ihtiyaçlarının karşılanmasında önemli bir yer tutan arşivlerin ve hizmetlerinin çağın gereklilikleri göz önünde bulundurularak yeniden ele alınması ve üzerinde düşünülmesi gereken bir konu olarak karşımıza çıkmaktadır.

Kaynakça

Atilla, A., Mansur, F., Uslu, D. (2015). Teknoloji kullanılabilirliği ve bireysel teknolojik hazır oluşun elektronik belge yönetim sistemi kullanımına etkisi: üniversite hastanesi çalışanları üzerinde bir uygulama. *İşletme Araştırmaları Dergisi*, 7, (2), 375-387.

Ayliz Demir, F. (2013). Değişen dünyada arşivlerin farklı amaç ve uygulamalarına bir bakış: Geleceğin arşivciliğine öngörüler. Yüksek lisans tezi. İstanbul: Marmara Üniversitesi

Dinçer, Ö., Fidan, Y. (1996). İşletme yönetimine giriş. İstanbul: Beta.

Kalkınma Bakanlığı. (2012). E-dönüşüm Türkiye Projesi birlikte çalışabilirlik esasları rehberi (Sürüm 2.1, (2012). Ankara: Kalkınma Bakanlığı Bilgi Toplumu Dairesi. (13 Eylül 2017 tarihinde http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Birlikte_Calisabilirlik_Esaslari_Rehberi_2.1.pdf)

Eminağaoğlu, M., Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir? Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11,* (4), 1-14.

ISO 27001. (2006). Bilgi teknolojisi – güvenlik teknikleri – bilgi güvenliği yönetim sistemleri– gereksinimler. Ankara: Türk Standartları Enstitüsü.

Kahveci, M., Yenen, S. (2014). Uluslararası bilgi sistemlerinde bilgiye erişim, bilgilerin depolanması ve teknik analizi. *Muhasebe ve Denetime Bakış, 14,*(42), 69-84.

Kalseth, K., Cummings, S. (2001). Knowledge management: Development strategy or business strategy?. Information Development, 17(3), 163-172.

Kandur, H. (2006). Elektronik belge yönetimi sistem kriterleri referans model (v.2.0). 21 Eylül 2017 tarihinde Devlet Arşivleri Genel Müdürlüğü web sitesinden erişildi: https://www.devletarsivleri.gov.tr/assets/content/Yayinlar/cumhuriyet-arsivi-yayinlar/ELEKTRON%C4%B0K%20BELGE%20Y%C3%96NET%C4%B0M%C4%B0%20S%C4%B0STEM%20KR%C4%B0TERLER%C4%B0%20REFERANS%20MODEL%C4%B0%20(V.2.0).pdf

Külcü, Ö., Çakmak, T. (2009). Elektronik belge yönetimi üzerine Inter PARES projesi ve Türkiye takımı faaliyetleri. *Bilgi Dünyası*, *10,* (2), 287-302.

Marcinkowski, S. J., Stanton, J. M. (2003, October). Motivation al aspects of information security policies. In Systems, Man and Cybernetics, 2003. IEEE International Conference on (Vol. 3, pp. 2527-2532). IEEE.

Mitnick, K. D., Simon, W. L. (2011). The art of deception: controlling the human element of security. John Wiley&Sons.

Odabaş, H. (2007). Elektronik belge yönetimi ve kamu kurum ve kuruluşları. Yayınlanmamış doktora tezi. Ankara: Ankara Üniversitesi. Önaçan. M.B.K,

Özdemirci, Fahrettin .(1999) Arşivlerimizin kurumsal yapılanma gereksinimleri, Bilginin serüveni: dünü, bugünü, yarını: Türk Kütüphaneciler Derneği'nin Kurulusunun 50. Yılı Uluslararası Sempozyum Bildirileri 17-21 Kasım 1999, Ankara / Yayını hazl. Özlem Bayram... (ve diğerleri). İçinde. 366-383.Ankara: TKD, İçinde,

Özdemirci, Fahrettin. "Belge Üretimi ve Kurumsal Bilgi Yönetimi" 21. Yüzyıla Girerken Enformasyon Olgusu Sempozyumu: Bildiriler (19-20 Nisan 2001:Hatay). Ankara: Türk Kütüphaneciler Derneği, 2001. İçinde, 179-186.

St. Clair, G. (2003). Knowledge management. Encyclopedia of Library and Information Science içinde (Vol. 2, 1486-1494). 2d ed. Ed. By Miriam A. Drake. New York: Marcel Dekker.

Şahin, A. (2010). Örgüt kültürü-yönetim ilişkisi ve yönetsel etkinlik. Maliye Dergisi, 159, 21-35.

Tipton H. F., Krause M. (2007). Information Security Management Handbook. Auerbach Publications.

Elektronik Belge Yönetim Sistemi'nde Belgelerin Uzun Süreli Korunmasına Dair Bir Yaklaşım Değerlendirmesi: Açık Arşiv Bilgi Sistemi Referans Modeli (OAIS)

An Approach Evaluation Regarding Records' Long-Term Preservation in Electronic Records Management System: Open Archival Information System Reference Model

Uzm. Mehmet Oytun CİBAROĞLU
Bursa Teknik Üniversitesi

Öz

Özellikle son 30 yılda giderek artan bir hızda gelişen bilişim teknolojilerinin en çok nüfuz ettiği alanların başında gelen belge yönetimi konsepti değişime uğramıştır. Belgelerin elektronik ortamda oluşturulması, düzenlenmesi, iletilmesi ve korunmasının sağlanması neticesinde iş verimi artmış ve organizasyonlar kurumsal bir yapıya kavuşmuştur. Özellikle EBYS kullanan organizasyonlar, bu sistemi kullanmayanlara göre daha efektif iş süreçlerine sahip olmuştur. Bunun nedeni de kurum içi temel bilgi iletimini sağlayan EBYS'de belgelerin çok daha hızlı oluşturulması ve gerektiğinde daha kolay bulunabilmesidir. Bu tür yazılımların içerisinde gömülü halde bulunan dijital arşiv depolama alanlarında belgelerin nasıl saklandığına dair sorular da günümüzde EBYS'ye geçmeye hazırlanan organizasyonları meşgul eden bir ayrıntıdır. Çünkü e-belgelerin içerik, bütünlük ve doğruluk bakımından hatasız ve herhangi bir eksikliğe neden olmayacak şekilde saklanması ispat hukuku açısından son derece önemlidir. Bunun için çeşitli model ve standartların oluşturulmasına ihtiyaç duyulmuştur. Bunlardan biri olan Open Archive Information System (OAIS), bilgi kaynakları içeren neredeyse tüm organizasyonların (çoğunlukla da kütüphane ve arşivlerin) sahip olduğu tüm dijital kaynaklarının uzun süreli depolanması için oluşturulan bir referans modeldir. Temel amacı; bilgi paketleri (SIP, AIP ve DIP) vasıtası ile bilgiyi korumak, uzun vadeli kalıcılığını güvence altına almak ve arşivlenmiş bilgiye sürekli erişimi sağlamaktır. Uzun süreli tam bir korumada saklama verilerinin XML paketi olarak kullanılması ve belgelerin PDF/A standardında e-imzalı ve zaman damgalı olarak korunması sıklıkla kullanılan bir uygulamadır. Bu çalışmada EBYS bağlamında belgelerin uzun süreli korunmasında OAIS bilgi paketleri (SIP, AIP ve DIP) vasıtası ile belgelerin XML tabanlı oluşturulduktan sonra EBYS yazılımı içerisinde gömülü halde bulunan dijital depolama alanına transferlerine dair bir model yaklaşımı değerlendirilecektir.

Anahtar sözcükler: *E-Arşiv, EBYS, OAIS, XML, Koruma*

Abstract

Especially in the last 30 years, at a growing pace, the concept of records management which is one of the areas where information technologies have penetrated the most, has changed. As a result of the creation, organization, transmission and preservation of documents in electronic form, job efficiency has increased and organizations have become institutionalized. Organizations using ERMS in particular have more efficient business processes than those who do not use this system. The reason is that the documents in ERMS, which provide basic information transmission within the organization, can be created much faster and can be found more easily when needed. The questions about how electronic records store in digital archive repository that embedded in such software is a detail that keeps organizations busy that is preparing for ERMS. Because preserving e-documents in terms of content, integrity, accuracy and wthout causing any incompleteness is extremely important for evidence law. That's why various models and standarts have been required. One of these Open Archive Information System (OAIS) is a reference model for long-term preservation for organizations (mostly libraries and arvhives) that includes of all type of digital resources. Primary aim is to preserve documents via information packages (SIP, AIP and DIP), to secure long-term permanence and to provide continuous access to archived information. It is a common implementation using preservation data as XML packages in long-term preservation and preserving documents with e-sign and time stamp. In this study, in the context of documents long-term preservation in ERMS, creating documents in XML based via OAIS Information Packages (SIP, AIP and DIP), a model will be evaluated approaching to transferring embedded digital storage in ERMS software.

Keywords: *E-Archive, ERMS, OAIS, XML, Preservation*

Giriş

Bilgi teknolojilerinin özellikle son 30 yılda hızlı gelişim göstermesi, belge ve dokümanların elektronik ortamda da üretilebileceği fikrini ortaya çıkarmıştır. Bununla birlikte, belgelerin yaşam döngüsü sonunda yine elektronik ortamda güvenli bir şekilde arşivlenebileceği de savunulmuştur. Üretilen çeşitli yazılımlar sayesinde bu işi yapabilecek programların ortaya çıkmasından sonra organizasyonlar, bazı faydaları nedeniyle bu programları zaman içinde kullanmaya başlamışlar ve tüm yazışmalarını bilgisayar ortamına taşımışlardır. Bu noktada ise konu bağlamında temel sorun olarak koruma işleminin elektronik ortamda nasıl yapılacağı tartışılmaya başlanmıştır. Elektronik ortamda üretilen ve saklanan belgeler nasıl sürekli korunacaktır? İçerik ilişkileri ve belge yapısı özellikleri bütün bir formda nasıl saklanabilir? vb. tarzında sorular ortaya çıkmıştır. Elektronik belgelerin, mevcut yazılımın içinde tüm içerik bilgileri ile tam bir koruma sağlanarak uzun süreli korunması, arşivleme ve gelecek kuşaklara bilgi aktarımı konusunda son derece önem arz etmektedir.

Organizasyonlarda elektronik bilgi ve belgelerin saklanmasının temel amacı; bunlara gerektiğinde hızlı bir şekilde erişimi sağlamak ve gelecek kuşaklara sağlıklı bir biçimde iletmektir. Bunun için de günümüzde yapılması gereken, elektronik arşivlemedir. Elektronik bilgi kaynaklarının korunması ve arşivlenmesi basılı kaynaklara nazaran farklılık arz eder. Bir fiziksel belgenin temel yapısal

özelliklerini korumak, entelektüel içeriğin korunmasını sağlamaktadır. Bilgilerin bulunduğu fiziksel ortam zarar görmedikçe, bilgiye erişmek mümkün olur (Tonta, 2002). Fakat elektronik ortamda oluşturulan belgelerin korunması ve arşivlenmesi ise oldukça karmaşıktır. Bu tür belgeler EBYS dışına çıkarılıp analog ortamda mı saklanmalı yoksa yazılımın içinde gömülü halde bulunan veritabanlarında saklanmasına devam mı edilmelidir? Aslına bakılacak olursa elektronik ortamların ömrü analog ortamlar olan kâğıt ve mikro fiş vb. ile karşılaştırıldığında daha kısadır. Manyetik ortam; 10 - 30 yıl, CD-ROM yaklaşık 100 yıl, kâğıt 100 yıl, mikro fiş ise 300 yıl boyunca verileri saklayabilmektedir. Ayrıca, elektronik belgelere tam erişim için multimedya yazılımını çalıştıran bilgisayar, iletişim ve ağ teknolojilerine gerek duyulmaktadır. Bu durumda elektronik belgelerin okunabilmesi için bilişim teknolojileri ürünlerine ihtiyaç bulunmaktadır. Bu da bize; bilgiye erişmek için hem mantıksal içeriğin hem de teknolojinin korunması gerektiğini göstermektedir (Tonta, 2002).

Elektronik bilginin korunması ve arşivlenmesi temel olarak kopyalama işlemine dayanmaktadır. Eski ortamlar üzerine kaydedilmiş bilgilerin, eski teknoloji kullanılmasından dolayı tamamen erişilemez hale gelmemesi için zaman zaman daha yeni ortamlara aktarılması gerekmektedir. Koruma ve arşivleme amacıyla yapılan kopyalama, "teknoloji yenileme" ya da "belge göçü" olarak adlandırılmaktadır (Preserving Digital Information, 1996). Daha geleneksel ortamlar üzerine kayıtlı bilgiler de elektronik ortamlara aktarılabilir. Fakat bunun için; belgelerin içerik özelliklerinin önceden tanımlanarak belirli bir algoritma ile kodlama işlemi yapılmalıdır. Başka bir deyişle dijitalleştirme işlemi gerekmektedir. Önemli bir diğer husus da bilginin bir ortamdan diğer ortama transferi sırasında çeşitli formatlama sorunları sonucu kayıpların ortaya çıkabileceğidir. Bir yazılımın daha güncel bir sürümü, bir önceki sürümde hazırlanan bilgi ve belgeleri tanımayabilir. Bu durumda ek yazılım maliyetleri ortaya çıkacaktır. Bu sorunların önüne geçebilmek için:

- Kopyalama için basit formatlar kullanılması;
- Görüntü dosyalarının sıkıştırılmadan korunması;
- Elektronik belgelerin yaratılması ve arşivlenmesi için aynı yazılımın kullanılması;
- Kaliteli ortamlar kullanarak her belgeden iki kopya arşivlenmesi;
- Donanım ve yazılım terfiinden önce bir arşivleme planı geliştirilmesi
- Yeni yazılımın arşiv kopyalarını okuyup okumadığının test edilmesi gerekmektedir (Tonta, 2002).

Bu çalışmanın amacı; elektronik belgelerin uzun süreli korunması ve saklanmasında, OAIS Referans Modeli yaklaşımını uzun süreli bir koruma modeline entegre ederek öznel bir değerlendirme yapmak ve bu alanda literatüre katkıda bulunmaktır.

Belge, Elektronik Belge, Belge Yönetimi ve EBYS

Belge: Köken olarak Latince documentum (doceō+mentum) kelimesinden gelir. Doceō fiili öğretmek anlamındadır (Oxford Latin Dictionary, 2005). Belge yönetimi alanında oluşturulan ilk uluslararası standart olan ISO 15489-1:2001'de; bir kuruluş ya da kişi tarafından kanuni yükümlülükler izlenerek veya ticari işlemlerde kanıt ve bilgi olarak yaratılan, elde edilen ve muhafaza edilen bilgiler[1] şeklinde tanımlanmıştır. Society of American Archivist (SAA) tarafından yayınlanan "A Glossary of Archival and Records Terminology" (Moses, 2005, s. 128) sözlüğünde ise doküman anlamında da tanımlanmıştır:

- Yazılı veya basılı herhangi bir çalışma;
- Çeşitli medya ortamlarında sabit olarak bulunan ancak resmi kaydın bir parçası olmayan bilgi veya veriler.

Yine belge yönetimi alanında yapmış olduğu çalışmalarla tanınan Hamza Kandur'a göre (2011, s. 3) belge; herhangi bir bireysel veya kurumsal fonksiyonun yerine getirilmesi için alınmış veya fonksiyonun sonucunda üretilmiş, içerik, ilişki ve form özellikleri ile ait olduğu fonksiyon için delil teşkil eden kayıtlı bilgidir.

Elektronik Belge: International Records Management Trust tarafından yayınlanan Terimler Sözlüğünde (Millar, 2009, s. 13-16) "Bir bilgisayar tarafından depolanabilir, iletilebilir veya işlenebilir dijital bir kayıt" ve "Sayısal bir formatta muhafaza edilen, yalnızca insan gözü tarafından kavranabilecek metin veya imajlara dönüştüren bir bilgisayar sistemi kullanılarak erişilen bir kayıt" olarak tanımlanmıştır. Dijital kayıtlar, optik disk gibi elektronik ve elektronik olmayan formatta kaydedilmiş kayıtları içermektedir.

Aydın ve Özdemirci'ye (2011, s. 106) göre ise elektronik belge; bilgisayar ya da diğer elektronik cihazlar aracılığıyla elektronik ortamda iş süreçleri sonucunda üretilen, arşivlenen, erişilen, iletilen ve imha edilen her türlü belgeyi ifade eder. Ayrıca dijitalleştirilmiş kağıt belgelerin, elektronik belge sayılabilmesi ve yasal açıdan gerçekliğinin olabilmesi için dijitalleşme sırasında değişime uğramadığına dair bir zaman damgası alması gerekmektedir. Böylece dijital belgenin gerçekliği ve bütünlüğü korunmuş olur (Aydın, 2010, s. 44)

Belge Yönetimi: International Records Management Trust (IRMT) tarafından yayınlanan "Glossory of Terms" (2009, s.14) sözlüğünde; "belgelerin önceden belirlenmiş kurallar, ilke ve teknikler ile sistematik kontrolü" olarak tanımlanmıştır. Daha kapsamlı bir ifade ile belge yönetimi; organizasyonların işlerini yürütmesi sırasında ürettikleri veya dışarıdan aldıkları belgelerin üretim kontrolünün sağlanmasına, dağıtımına, erişimine, dosyalanmaları ve imha

[1] Standartta "Belge" terimi "Record" olarak kullanılmıştır.

edilmelerine yönelik, her çeşit organizasyonda uygulanabilecek bir yönetim sistemidir (Odabaş, 2005 s. 2). Bu ifadeler ışığında belgelerin daha etkin üretimi, düzenlenmesi, dağıtımı, imha edilmesi ve fiziksel arşivlere gönderilmesi gibi unsurlar bağlamında belge yönetimi, bir kurum veya kuruluşun idari yapısı içindeki alt yönetim birimlerinden biri olarak karşımıza çıkmaktadır. Bu sebeple belge yönetimi ve kurumsal yönetimin, bir organizasyonda birbirinden ayrılmaz ve direkt ilişkide olan prensip ve yöntemlere sahip olduğu söylenebilir. Belge yönetiminin temel kurumsal amaçları arasında; kurumsal kaynakların nasıl sağlandığının ve kullanıldığının belgelenmesi, kurumun ve kurum çalışanlarının haklarının korunması, kurumun tabi olduğu mevzuata uygun davranıldığının belgelenmesi ve tarihsel süreç içerisinde kurumsal devamlılığın izlenebilmesi bulunmaktadır (Kandur, 2011 s.3). Bu amaçlar, kurumlar açısından belge yönetiminin hayati bir fonksiyona sahip olduğunu göstermektedir. Çünkü resmi olarak yapılan işlemler, sayılan amaçlar doğrultusunda hukuki sonuçları ortaya çıkarmaktadır.

Elektronik Belge Yönetim Rehberi'nde (2004) bir belge yönetiminde olması gereken özellikler 4 başlık altında toplanmıştır:

- **Güvenilirlik:** Belgeler, güvenilir ve orijinal olan bilgileri içermelidir. Güvenilirliğin önemli bir özelliği de hukuki açıdan kabul edilebilirliğidir. Örneğin; belgelerin mahkemelerde kanıt ve delil olarak kabul edilip edilmeyeceği gibi.
- **Tamamlayıcılık:** Belgeler, uzun süreli fayda sağlayabilmek için gereken tüm bilgilere sahip olmalıdır. Bunun için de belgelerin ilgili üstverilerini saklamak gerekmektedir. Üstveriler, belgelerin kurumlarda etkinliğini ve diğer belgelerle olan ilişkisini gösteren veri hakkında veridir. Üstveri, temelde belgelerin kolayca bulunmasını sağlar. Ayrıca üstveriler, bir kaydın yaratıcısı, oluşturulma tarihi ve kaydın ait olduğu kayıt dizisi gibi unsurları içerir.
- **Erişilebilirlik:** Belgeler, gereksinimleri ve diğer tüm ilgili tarafların ihtiyaçlarını karşılayacak bir şekilde erişilebilir olmalıdır. Bazı belgelerin hemen erişilebilir olması gerekebilir, bazılarına da hemen erişim ihtiyacı olmayabilir. Devlet tarafından kamuya açık olmayan kategorilere ayrılmadıkça, belgelerin kamuya açık olduğu kabul edilmektedir.
- **Dayanıklılık:** Belgeler, belirlenmiş kayıt tutma süreleri için erişilebilir olmalı ve uygun olduğunda "kalıcılık sağlamak için" fiziksel bir ortamda saklanmalıdır (Rounds ve Horton, 2004).

Elektronik Belge Yönetim Sistemi (EBYS): Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli'nde (v2.0) (2006); *kurumların gündelik işlerini yerine getirirken oluşturdukları her türlü dokümantasyonun içerisinden, kurum aktivitelerinin delili olabilecek belgelerin ayıklanarak bunların; içerik, format ve ilişkisel özelliklerini korumak ve bu belgeleri üretimden nihai tasfiyeye kadar*

olan süreç içerisinde yönetmek olarak tanımlanmıştır. İngiliz Ulusal Arşivleri ise EBYS'yi şu şekilde tanımlamaktadır: *İlişkisel bir veritabanında saklanan tüm elektronik kayıtları yönetmek için kullanılan bir bilgisayar program dizisi olup; erişim denetimleri, sistem kombinasyonunu kullanarak kullanıcı tarafından oluşturulan üstveri ve belgeleri imha etme gibi daha birçok çeşitli foksiyonlar sağlayan bir yapıdır.* Bu tanımlardan hareketle bir EBYS'nin sahip olması gereken özellikler şu şekilde açıklanabilir:

- **Güvenilirlik**: Belgeleri yönetmek için kullanılan herhangi bir sistem, prosedürlere uygun olarak sürekli ve düzenli bir şekilde çalışabilir olmalıdır.

  Bir elektronik belge yönetim sistemi;

  a) Kapsadığı iş faaliyetleri bağlamında tüm belgeleri düzenli olarak tutmalı,

  b) Belgeleri, yaratıcısının iş süreçlerini açıkça gösteren bir şekilde organize etmeli,

  c) Belgeleri, yetkisiz değiştirmeye veya silinmesine karşı koruyabilmeli,

  d) Kayıtlarda belgelenen işlemlerin birincil bilgi kaynağı olarak her zaman bu işlevini yerine getirmeli,

  e) İlgili tüm kayıt öğelerine ve üstveriye hızlı erişimi sağlamalıdır.

  Sistemin güvenilirliği, ilgili sistemlerin çalışma kayıtlarının oluşturulması ve muhafaza edilmesi yoluyla belgelendirilmelidir. Bir EBYS, değişen iş gereksinimlerine duyarlı olmalı ancak sistemdeki herhangi bir değişikliğin, sistemde bulunan belgelerin karakteristikleri üzerinde etkisi olmamalıdır. Benzer şekilde, belgeler bir EBYS'den diğerine transfer edilmek istendiğinde, aktarım, belgelerin özelliklerini olumsuz olarak etkilemeyecek bir şekilde gerçekleştirilmelidir.

- **Bütünlük:** Erişim izlemesi, kullanıcı doğrulaması, yetkilendirilmiş imha ve güvenlik gibi kontrol tedbirleri; yetkisiz erişim, imha, değiştirme ya da belgelerin ortadan kaldırılmasını önlemek için uygulanmalıdır. Elektronik belgeler için kuruluş; herhangi bir sistem arızasının, üst versiyonlara geçişin veya düzenli bakımın, belgelerin bütünlüğünü etkilemediğini ispatlamaya gerek duyabilir.

- **Uygunluk:** EBYS; mevcut mevzuat ortamı ve kuruluşun faaliyet gösterdiği topluluk beklentilerinden kaynaklanan tüm gerekliliklere uygun olarak yönetilmelidir. Belgeleri oluşturan personel, bu gerekliliklerin iş süreçlerini nasıl etkilediğini anlamalıdır. Belge yönetim sisteminin, bu gibi gerekliliklere uygunluğunun düzenli olarak

değerlendirilmesi ve bu değerlendirmenin delil amacıyla saklanması gerekir.

- **Kapsayıcılık:** EBYS, organizasyondaki tüm işletme faaliyetlerinden veya organizasyonun bir bölümünden kaynaklanan tüm kayıtları (doküman, belge vb.) yönetmelidir.
- **Sistematiklik:** Belgeler sistematik olarak oluşturulmalı, muhafaza edilmeli ve yönetilmelidir. Belgelerin oluşturulması ve bakım uygulamaları, iş sistemleri ve EBYS'nin birlikte tasarlanıp yönetilmesi yoluyla sistematik bir hale getirilmelidir. Bir EBYS, yönetim için doğru bir şekilde oluşturulmuş politikalara, önceden belirlenmiş sorumluluklara ve resmi metodolojilere sahip olmalıdır (ISO 15489:1, 2001)

E-Belgelerin Arşivlenmesi

Uzun dönem arşivleme açısından, uygun standartların göz önünde bulundurulması, özel olmayan veri formatlarının kullanılması, zorunlu standartlarla uyumlu olarak gerekli dokümantasyon ve üst verinin sağlanması büyük önem taşımaktadır (Hollier (2001)'den aktaran Aydın ve Özdemirci, 2011, s. 108). E-belgelerin uzun süreli korunması ile ilgili olarak birden çok çözüm bulunmaktadır. Janée, Methana ve Frew (2008) tarafından Amerikan Kongre Kütüphanesi NDIIPP programı kapsamında kurulan Ulusal Coğrafi Dijital Arşivi için geliştirilen NGDA Veri Modeli, Duranti (2005) tarafından InterPARES projesi kapsamında oluşturulan Koruma Zinciri Modeli (The Chain of Preservation Model) ve Paquet ve Viktor (2007) tarafından kültürel mirasların 3 boyutlu tarayıcı vasıtasıyla bilgisayara aktarılıp arşivlenmesi için geliştirilen Üç Boyutlu Uzun Süreli Koruma Modeli (3-D Long-Term Preservation Model) bu çözümlere örnek olarak verilebilir. Bu çözümlerin ortak yönü; dijitalleştirilerek elektronik ortama aktarılan basılı materyallerin sonradan e-belge'ye dönüştürülerek uzun süreli koruma modellerinin oluşturulmasıdır. Fakat EBYS'lerde hâlihazırda sistem içinde oluşturulan belgelerin sistem içinde gömülü veritabanlarında uzun süreli saklanabilmesi için farklı yöntemlerin bir arada uygulanması gerekebilir.

Bu tip dijital arşiv oluşturma hususunda, yazılım ve donanım önem kazanmaktadır. Donanımın, ilerleyen yıllarda artması muhtemel belge yoğunluğu göz önüne alınarak konumlandırılması; yazılım unsurlarının da periyodik dönemler halinde güncellenmesi sağlanmalıdır.

Çeşitli özel ve gizli belgeler şifreli formda arşivlenmesi gerekmektedir. E-belgelerin ise güvenlikle ilgili yasal ve idari düzenlemelerin öngördüğü çerçevede şifrelenmiş formda saklanması gereklidir. Elektronik belgelerin uzun dönem arşivlenmesi açısından zaman içindeki güvenirliliğini ve kullanılabilirliğini sağlamak için taşıma, koruma, üst veri ve XML (Extensible Markup Language -

Genişletilebilir İşaretleme Dili) gibi araçlar, yalnızca belgelerin korunmasına yardımcı olmaz; aynı zamanda gerçek değerlerinin fark edilmesinde destekleyici rol oynar. Organizasyon, elektronik belgelerle ilgili bir koruma planına sahip olmalı ve bu plan, yazılım ve donanımdaki değişiklikleri, depolama ortamlarındaki kısıtlamaları ve bilginin potansiyel kullanım değeri gibi hususları içermelidir (Rounds ve Horton, 2004, s. 2).

Elektronik Belgelerin Uzun Süreli Korunması

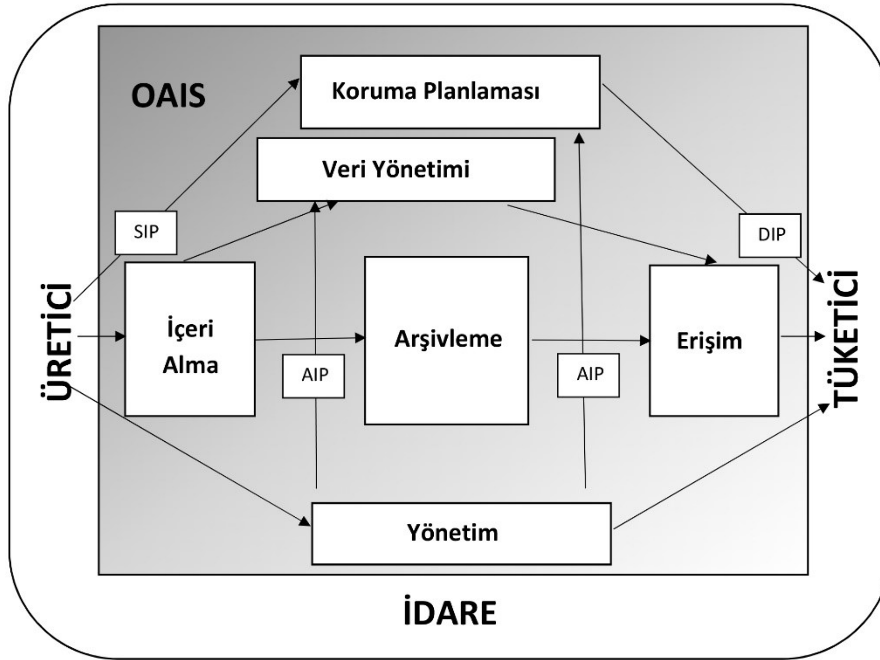
Kurumlar açısından elektronik belge yönetimi içerisinde arşivleme sisteminde öne çıkan ihtiyaç; resmi anlamda oluşturulan elektronik belgelerin değiştirilmeden yani tamlık, bütünlük ve gerçeklik açısından korunmasıdır. Bu ihtiyacın ortaya çıkmasında, aktarım sırasında ortaya çıkabilecek hata ve yapının bozulması, belge üzerinde yapılabilecek değişiklik ve kayıp olma ve zarar görme ihtimallerinin önemli sebepler olduğunu ifade edilmektedir (Aydın ve Özdemirci, 2011, s. 122). Elektronik belgelerin uzun süre korunmasını, gerçekliğini ve bütünlüğünü koruyacak ve kontrolünü sağlayacak güncel teknolojik çözümler şu şekilde sıralanabilir:

- **Kriptografik Teknikler:** Elektronik belgelerin aslına uygunluk ve bütünlüğünün sağlanması ve kontrolü için geliştirilen algoritmaları temel alır. Bunun yanında belgenin iletimi sırasında oluşabilecek değişikliklere karşı oluşturulan sağlama (hash) algoritmaları da bu kapsamda düşünebilir.
- **Zaman Damgası:** Elektronik belgenin bütünlüğünün sağlanması bağlı olarak belgenin oluşturulduğu zamanı kesin bir şekilde tespit edilip kayıt altına alınmasını sağlar. Kurumlarda kullanılan sistemler yerine güvenilir bir üçüncü taraftan alınan zaman kayıtları ile belgenin düzenlenme tarihi kesin olarak kayıt altına alınmış olur.
- **Elektronik İmza:** Elektronik belge içerisine eklenen e-imza, EYBS ile doğrulama işlemine tabi tutularak hata alıp almama sonucuna göre belgenin değiştirildiğini veya tahrip edildiğini kontrol edebilmektedir. Diğer tekniklerden farklı olarak e-imza EBYS içerisinde kullanılır ve elektronik belgedeki imza doğrulaması bu yapı içerisinde gerçekleştirilir (Sproull ve Eisenberg, 2005, s. 60)

OAIS Referans Modeli

Open Archive Information System – Açık Arşiv Bilgi Sistemi; The Consultative Committee for Space Data Systems (CCSDS) - Uzay Veri Sistemleri Danışma Komitesi tarafından uzay görevleri sonucunda üretilen dijital verilerin uzun vadeli

depolanması için resmi standartlar geliştirme çabaları sonucu oluşturulan bir referans modelidir (Lavoie, 2014, s. 2). Model; dijital bilginin uzun vadeli korunması ile ilgili olarak bir sistemin temel fonksiyonel bileşenlerini tanımlar, sistemin ana iç ve dış sistem arayüzlerini detaylandırır ve sistem tarafından yönetilen bilgi nesnelerini karakterize eder. Referans modeli ayrıca, bir arşiv sisteminin karşılaması beklenen bir dizi asgari koşulları da belirtir. OAIS modelini uygulayan arşivlerin iki temel fonksiyonu vardır: Bilgiyi korumak, uzun vadeli kalıcılığını güvence altına almak ve arşivlenmiş bilgiye sürekli erişim sağlamaktır (Lavoie, 2014, s. 7).



Şekil 1: OAIS Fonksiyonel Modeli
Kaynak: (OAIS Reference Model Introductory Guide, 2014, s. 12)

Şekil 1'de görülen OAIS Referans Modeli'nin çeşitli mantıksal alt alanları aşağıdaki gibi tanımlanabilir:

İçeri Alma (Ingest): Bu işlev, OAIS'in üretici veya dağıtıcılar arasında bir arayüz olarak işlev görür ve gönderilen bilgilerin saklanmak üzere kabul edilmesi için oluşturulan hazırlama sürecini kapsar (Lavoie, 2014, s. 12). Bu varlığın işlevleri; SIP'lerin alınması, SIP'lerde kalite güvencesi yapılması, arşiv verisinin formatlaması ve dokümantasyon standartlarına uygun bir Arşiv Bilgi Paketi (AIP) oluşturulması, arşiv veritabanına dahil edilmek üzere

AIP'lerden Tanımlayıcı Bilgi'nin çıkartılması ve arşiv alanıyla ve veri yönetimi ile ilgili güncellemelerin koordine edilmesidir (Sawyer, 2001).

Arşivleme: Bilgilerin SIP olarak içeri alınmasından sonra AIP formatına dönüştürülen dijital verilerin uzun süreli depolama ve bakımını sağlayan varlıktır (Lavoie, 2014, s. 12). Fonksiyonları; içeri alınan SIP'leri AIP'e dönüştürmek ve bunları kalıcı saklama alanına eklemek, saklama hiyerarşisini yönetmek, arşiv varlıklarının saklandığı ortamı sürekli çalışır halde tutmak, rutin ve özel hata denetimi yapmak, felaket kurtarmayı sağlamak ve AIP'lere erişimi sağlamaktır (Sawyer, 2001).

Veri Yönetimi: Arşivi yönetmek için yönetimsel verileri ve belge topluluğunu sınıflandıran ve tanımlayıcı bilgiye erişimi sağlamak ve korumaya yönelik işlevleri sağlar. Arşiv veritabanını yönetmek, veritabanı güncellemelerini gerçekleştirmek, sonuç kümeleri oluşturmak için veri yönetimi üzerinde sorgular gerçekleştirmek, bu sonuç kümelerinden raporlar üretmek, fonksiyonları arasındadır. Sistem performans verileri veya erişim istatistikleri gibi OAIS'in iç sistem operasyonlarını destekleyen idari verileri de yönetir (Sawyer, 2001).

Koruma Planlaması: OAIS'in koruma stratejisini haritalamaktan ve aynı zamanda OAIS ortamında gelişen koşullara yanıt olarak bu stratejiyi uygun revizyonlara dönüştürmekten sorumludur. Koruma planlama hizmeti, depolama ve erişim teknolojilerinde meydana gelen yenilikleri ve bilgiye erişimdeki çeşitli riskleri tanımlamak amacıyla dış ortamı denetler (Lavoie, 2014, s. 13).

Erişim: Tüketicilere OAIS arşivi içinde bulunan bilgi ve belgelerin yerini belirtir, belge edinme talebi süreçlerini ve hizmetleri yönetir. Erişim, arşivlenmiş içerikle ilişkili güvenlik ve erişim kontrol mekanizmalarının uygulanmasından da sorumludur. (Lavoie, 2014, s. 13)

Yönetim: Yönetim fonksiyonu, OAIS'in günlük işlemlerini yönetmenin yanı sıra diğer OAIS işlevlerinin faaliyetlerini koordine etmekten sorumludur. Yönetim fonksiyonu ayrıca, arşivleme ve erişim sistemlerinin denetimini yapmak, sistem performansını izlemek ve sistemdeki güncellemeleri uygun şekilde koordine etmekle sorumludur. Yönetim, OAIS'in iç ve dış etkileşimlerinin merkezi olarak hizmet verir (Lavoie, 2014, s. 13).

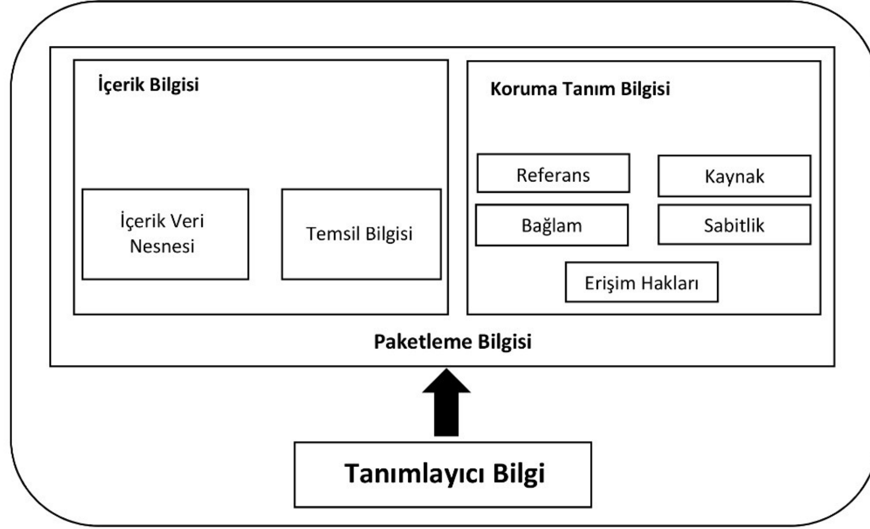
OAIS Bilgi Modeli

OAIS fonksiyonlarını; mantıksal bir bilgi modeli altında çeşitli bilgi paketleri (Information Packages - IP) vasıtasıyla yerine getirir. Bilgi modeli; arşiv sistemi

içindeki bilgi yapısının kavramsallaştırılması ile oluşmuştur. Bir bilgi paketi, korunan nesne (belge) ile birlikte, uzun vadeli koruma, erişim ve anlaşılabilirliği tek bir mantıksal pakete bağlamak için gerekli üstverileri içerir. Bilgi paketinin üç türü vardır: Gönderim Bilgi Paketi, Arşiv Bilgileri Paketi ve Dağıtım Bilgi Paketi (Lavoie, 2014, s. 14).

Gönderi Bilgi Paketi (Submission Information Package – SIP): Gönderi Bilgi Paketi (SIP) özetle, üretici'den OAIS'e aktarılan bilgi paketidir. Üretici; gerek basılı ortam materyalleri(kitap, tez, süreli yayın vb.) gerekse elektronik ortamda üretilen dijital belgeleri (e-belge, e-doküman vb.) sağlayan bir oluşum olabilir. EBYS açısından bir SIP; dijitalleştirme yoluyla harici ortamdan sistem içine alınan belge veya hâlihazırda sistem içinde hazırlanan bir e-belgedir. SIP kavramı, bilginin üretici tarafından sunulduğu şekliyle saklanamayacağını vurgular. Üreticiden sağlanan SIP, olduğu gibi OAIS modelinde arşive gönderilmez. Bir belge, birden çok SIP vasıtası ile sağlanan içeriğin bir araya toplanması sonucunda da oluşabilir (Lavoie, 2014, s. 14).

Arşiv Bilgi Paketi (Archival Information Package – AIP): Arşivlenen bilgi ve ilişkili üstveriler, arşiv sistemi içinde tek bir mantıksal paketi temsil eder. OAIS'te, üstveriyi bilgi nesnesinin kendi içine gömmek ve birleştirilmiş bir nesneyi tek bir bit akımı olarak depolamak gibi herhangi bir fiziksel ilişki biçiminin muhafaza edilmesine ilişkin bir gerek yoktur. Arşivlenen bilgilerin saklanması ve üstverisi OAIS uygulayıcılarına bırakılmıştır. AIP, Arşiv Bilgi Birimi (AIU) ve Arşiv Bilgisi Koleksiyonu (AIC) olarak 2'ye ayrılır. Bir AIU, içeriği ve üstveriyi tek bir "atomik nesne" (örneğin; tek bir dijital film veya e-kitap) için depolarken, AIC ayrı bir koleksiyonda gruplandırılmış birden fazla AIU'dan oluşmaktadır. Tek bir AIU birden fazla AIC'nin parçası olabilir. Buna ek olarak, AIC'nin kendisi de daha geniş bir AIC'nin bir parçası olabilir. AIC belirli bir koruma tekniği gerektiren nesneleri bir araya getirebilir. Kısacası AIC', bir OAIS tipi arşivdeki AIU'nun üst kavramıdır denilebilir. Yani AIU, AIC'yi açıklayan üstverilerdir (Lavoie, 2014, s. 16). Arşiv Bilgi Paketi, şu bölümlerden oluşur:



Şekil 2: Arşiv Bilgi Paketi
Kaynak: (OAIS Reference Model Introductory Guide, 2014, s. 16)

İçerik Veri Nesnesi: Bir AIP'in oluşturulması, İçerik Veri Nesnesi ile başlar. İçerik Veri Nesnesi herhangi bir materyal olabilir (metin, görüntü, video, veritabanları, bilgisayar programları - hatta toprak örnekleri veya fosiller gibi fiziksel malzemeler). İçerik Veri Nesnesi tek ve bağımsız bir nesneden oluşabilir (örneğin PDF formatında bir belge, HTML dosyaları ve GIF veya JPEG dosyaları). (Lavoie, 2014, s. 16).

Temsil Bilgisi: İçerik Veri Nesnesi'ne ait daha detay bilgileri içeren alandır. İçerik Veri Nesnesini oluşturan bit dizilerini oluşturmak ve anlamak için gerekli bilgileri içerir. İçerik Veri Nesnesinin yorumunu da özetleyebilir. Temsil bilgileri, iki tipe ayrılır: Yapı Bilgisi ve Semantik Bilgi. Yapı Bilgisi, bitleri anlaşılır bilgiye dönüştürür ve çeşitli kavramlar ve veri yapıları arasındaki eşleşmelere, yani bir resim, metin vb. gibi etkileşimli bir içerik bilgisine atıfta bulunur. Genel olarak, Yapı Bilgileri dijital nesnenin biçimini tanımlar. Semantik Bilgi ise, İçerik Veri Nesnesinin anlamını veya yorumlanmasını netleştiren bilgilerdir. Sözlük ve kullanıcı belgeleri, Semantik Bilgi'ye örnektir. Temsil bilgisi; METS şeması, XML, SGML standardı vb. alt bilgi paketlerinden oluşabilir (Lavoie, 2014, s. 16).

Koruma Tanım Bilgisi (PDI): İçerik Bilgilerinin uzun süre tutulması ek üstverileri gerektirir. Bu üstveriler, Koruma Tanım Bilgileri (Preservation

Description Information – PDI) olarak adlandırılır. Referans modeline göre PDI, İçerik Bilgilerinin önceki ve mevcut durumlarını tanımlamak, için oluşturulmuştur. (OAIS, 2012, 4-29). PDI beş bileşenden oluşur:

- **Referans Bilgileri**: OAIS'in iç sistemlerindeki İçerik Bilgisinin yanı sıra OAIS'in dışındaki kurumlar ve sistemlerdeki bilgileri de benzersiz bir şekilde tanımlar. Örnek; ISBN.
- **Bağlam Bilgisi**: İçerik Bilgisinin diğer nesneler ile olan ilişkilerini açıklar.
- **Gelişim Bilgisi**: İçerik Bilgisinin geçmişini, içeriğini veya değişikliklerini korumak için yapılan işlemleri belgeler.
- **Dayanıklılık Bilgisi:** İçerik Bilgilerinin belgelenmemiş bir şekilde, tam kontrol toplamları, dijital imza ya da dijital filigran gibi özgünlük veya bütünlük onaylama mekanizmaları ile değiştirilmemesini sağlar.
- **Erişim Hakları Bilgisi:** Koruma ve erişim ile ilgili koşulları veya kısıtlamaları belgelemektedir. Örnek olarak; lisans koşulları, yetkili erişim iznine sahip kişilerin belirli bir IP adresi aralığının tanımlama bilgileri ve korunma şartlarını ve koşullarını içeren bilgiler (Lavoie, 2014, s. 18) verilebilir.

Birlikte ele alındığında, İçerik ve Koruma Tanım Bilgisi, arşivlenmiş dijital içeriğin oluşturulup anlamlandırılabilmesi için gerekli üstveriyi, korunmasını, özgünlüğünü ve yaygınlaştırılmasını sağlar.

Paketleme Bilgisi: İçerik ve Koruma Tanım Bilgisini tek bir mantıksal pakete bağlamak için kullanılır. Daha spesifik olarak, bu bilgi bileşenlerinin tümünü AIP altında birleştirerek bunları tanımlama ve arşiv sistemi içerisinde tek bir mantıksal birim olarak konumlandırmaya yarar. Paketleme Bilgileri, dizin ve dosya adları gibi temel bilgileri veya METS gibi daha ayrıntılı paketleme şemalarını içerebilir (Lavoie, 2014, s. 18).

Tanımlayıcı Bilgi: OAIS'in, tüketicileri tarafından içerik bulgularının keşfedilmesini ve alınmasını destekleyen bilgidir. Örneğin; Tanımlayıcı Bilgi, İçerik ve Koruma Bilgilerinden türetilen ve arşiv kullanıcılarının keşfetmesini kolaylaştırmak için OAIS tarafından muhafaza edilen bir Dublin Çekirdek üstverisi biçiminde olabilir. (Lavoie, 2014, s. 18).

Dağıtım Bilgi Paketi (Dissemination Information Package – DIP): Dağıtım Bilgi Paketi, erişim durumunda olan belgelerin, çeşitli sorgular ile saklama alanından çıkartılıp tüketicilerin (son kullanıcılar) arama yapıp belgenin gösterimini sağlayacak şekilde bilgi paketlerinden oluşur. DIP kavramı, OAIS tarafından Tüketiciye dağıtılan bilgi paketinin şekil veya içerik bakımından arşiv deposunda bulunan bilgilere göre farklılık gösterebileceğini vurgular.

Bunun temel nedeni gösterimi konusunda bazı kısıtlar bulunan özel belgelerin çeşitli hukuki vb. durumlar gereği kullanıcılara iletilmemesidir (Lavoie, 2014, s. 15).

OAIS Referans Modeli bağlamında EBYS'de belgelerin uzun süreli korunmasında; uygulamanın içinde bulunan arşiv alanlarına transfer edilecek belgelerin arşivsel değerlerine göre ayrılması ve bundan sonra arşive gönderilecek e-belgelerin çeşitli koruma yöntemleri uygulanarak (XML gibi) paketler halinde depolama alanlarında saklanması önemlidir. Sistem tasarlama aşamasında, her bir belgenin üretimi ve tanımlamasıyla ilgili sistematik bir şekilde saklama sürelerinin ve imha tarihlerinin belirlenmesi, güvenli erişim ve koruma, belli belgelere erişimin kısıtlanması ve kimin yetkili olduğunun belirlenmesi gibi konularda kararlar alınmalıdır. (Shepherd, 1994, s. 42).

Sistem Mimarisi

Uzun süreli koruma sağlayan arşiv sisteminin mimarisi en az üç ana katmandan oluşmalıdır:

- Uygulama Katmanı;
- Orta (Özel Yazılım) Katman;
- Arşivleme Katmanı

Uygulama katmanı, web ya da portalın yanı sıra masaüstü uygulamalarını barındırır. Uygulamalar standartlaştırılmış uzun vadeli koruma biçimlerine (örneğin, PDF/A ve XML) uygun formatlarda arşivlenecek belgeler oluşturmak için kullanılmalıdır. Uzun vadeli koruma üzerinde imza doğrulamasını etkinleştirmek için, elektronik imza geçerliliği doğrulama verilerinin, yani kanıtın imza ile birlikte, arşivlenmesi önerilir. Güvenilir görüntüleme, elektronik olarak imzalanmış kayıtların izlenmesinde kullanılır ve gelişmiş bir elektronik imza uygulamaların güvenilir bileşenleri olarak işlev görürler.

Orta katman, uygulamaların arşivleme deposuna erişimini denetleyen standart ve güvenli bir ağ geçididir. Bu katman mantıksal olarak uygulama katmanındaki uygulamaları uzun vadeli koruma depolama alanından ayırır. Yazma, değiştirme veya silme gibi tüm işlemler bu katman aracılığıyla yapılır. Elektronik imza oluşturma, doğrulama, elektronik olarak imzalanmış arşiv bilgi paketlerini doğrulama, sertifika doğrulama, karma değer hesaplama gibi kanıtların korunması için gerekli kriptografik işlevlerin yanı sıra zaman damgalarının talep edilmesi ve doğrulanmasından da sorumludur.

Arşivleme katmanı, arşivlenen kayıtların uzun vadeli depolanması için kullanılan katmandır. Ana ve uzaktan depolama birimini içerir. Bulut depolamanın teknik ilkeleri bu alanda da geçerlidir.

Elektronik Veri Güvenliği (Electronic Data Safe – EDS)

Resmi belgelerin elektronik olarak güvenli bir şekilde depolanması bağlamında konseptin açıklaması, dijital olarak imzalanmış belgelerin doğruluğunun ve bunların güvenilirliğin uzun vadede nasıl korunabileceğini anlamamıza yardımcı olacaktır.

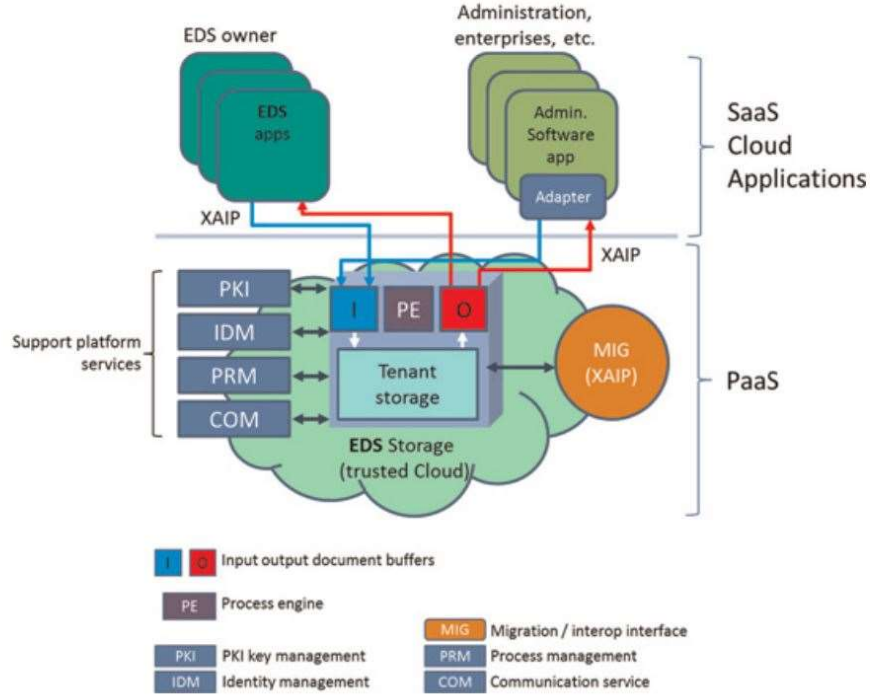
Deussen ve diğerleri (2012) EDS'yi, resmi belgelerin güvenilir bir saklama ortamı bileşeni olarak tanımlamaktadır. Bir EDS'nin fonksiyonları; elektronik ortamda oluşturulan resmi belgelerin güvenli bir biçimde uzun süreli korunması ile yönetim, kurumlar ve kişiler arasında elektronik iş akışları oluşturarak belge iletişimi sağlamaktır. Kullanıcılar kendi bölümlerinde yalnızca kendi EDS'lerine erişebilir ve bunu yaparken güvenli şifreli iletişim ve kimlik doğrulama sağlayan özel bir uygulamaya ihtiyaç duyarlar. Belgelerin bir bulut arşiv altyapısında güvenilir bir şekilde depolanması fikri EDS'nin temelini oluşturur. Ancak belgelerin birkaç bulut depolama sağlayıcısı arasında parçalanarak dağıltıldığı bir mekanizma tanımlayarak, yetkisiz kişilerin orijinal belgeye erişimini engeller (Breitenstrom, Brunzel ve Klessmann 2008).

EDS'deki veriler şifrelidir ve bu nedenle sağlayıcı tarafından görünür olmadığından, "veri koruma bariyeri" düşük kabul edilebilir ve uygulanan ilke veri anonimleştirme olarak nitelendirilebilir.

EDS sisteminin ana bileşeni EDS saklama alanıdır. Saklama alanı; depolama, erişim ve yönetim işlevleri sağlayan bulut tabanlı bir altyapıdır ve EDS kullanıcısının geçici bir saklama alanında belgelerini tutar. Erişim, yetkilendirme ve kullanım için bazı bileşenler barındırır.

Gidi (I) ve çıktı (O) bileşenleri, EDS içine alınması için yetki gerektiren belgelerin depolandığı alanı yönetmekten veya süreç motorunun (PE) belgelerin aktif kullanımını yönettiği zaman, kullanıcılara ulaştırılmasından sorumludur.

EDS'de kullanılan belge temsil biçimi, biçimlendirilmiş XML Arşiv Bilgileri Paketi'dir (XAIP). XAIP veya Evrensel Nesne Biçimi (Universal Object Format – UOF) gibi uzun süreli koruma verisi biçimleri genellikle veri ve üstverilerden oluşan bir kombinasyonu içerir.



Şekil 3: EDS Bileşenleri
Kaynak: (Deussen vd. 2012, s. 45)

Örneğin; XAIP, bir arşiv sistemi için tasarlanmıştır ve yapısı, Federal Bilgi Güvenliği Ofisi'nin (Kriptografik Olarak İmzalanan Belgelerin Kanıtlarının Korunması, 2011) teknik yönergesine dayanmaktadır. Arşiv Bilgileri Paketi (AIP), verileri ve ilgili üstverileri içeren bir XML dosyası iken, UOF; Üstveri Kodlaması ve İletim Standardı'nı (METS) temel alan verileri ve üstverileri iki ayrı dosyada (Potthoff, Marius ve Sebastian, 2013, s. 28) tutan bir veri biçimidir.

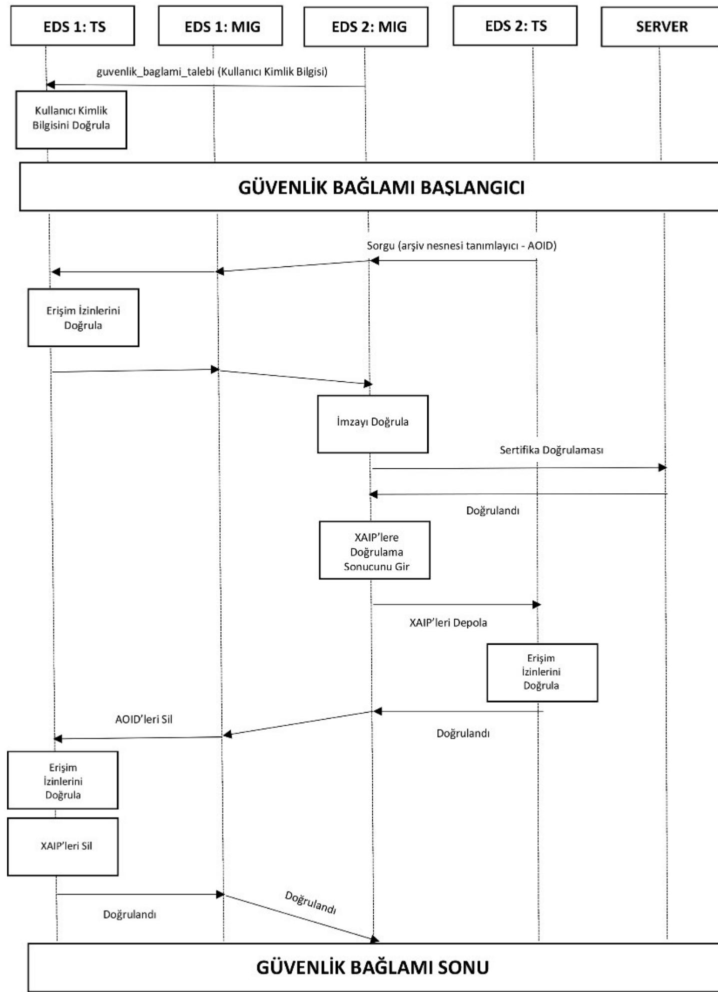
Bir XAIP dört bölümden oluşmaktadır:

a) XAIP'in mantıksal yapısı hakkında bilgi içeren arşiv paketi başlığı;
b) İçerik verisinin işlem ve arşivleme bağlamının tanımıyla birlikte üst bilgi;
c) Şifrelenmiş belgeleri içeren içerik verisi;
d) Elektronik imza, dijital sertifika, elektronik imzaları doğrulamak için gerekli bilgilerin yanı sıra dijital zaman damgalarını içeren sertifika bölümü.

Belgelerin Başka Bir Elektronik Arşive Taşınması

Uzun süreli koruma sırasında, EDS hizmeti sağlayan bir sunucunun zarar görmesi veya geri dönülemeyecek şekilde hasar alıp yedek verilere erişilememesi riskine

karşı, e-belgeler EDS altyapısı sağlayan başka bir sunucuya aktarılabilmelidir. Bu nedenle EDS mimarisinde geçiş arayüzü bulunmaktadır. Başka bir deyişle belgelerin transferinin sağlanabilmesi için bir alan bulunmaktadır. Korunan e-belgeler, kanıt olarak kullanılabilecek veriler içerdiğinden dolayı, bir sunucudan diğerine göçü sırasında, özgünlüğünü ve bütünlüğünü korumak için elektronik olarak imzalanması ve hemen akabinde zaman damgası alması gerekir; bu işlemler ilgili kanun ve yönetmelikler çerçevesinde yapılmalıdır (Deussen vd., 2012, s. 82).



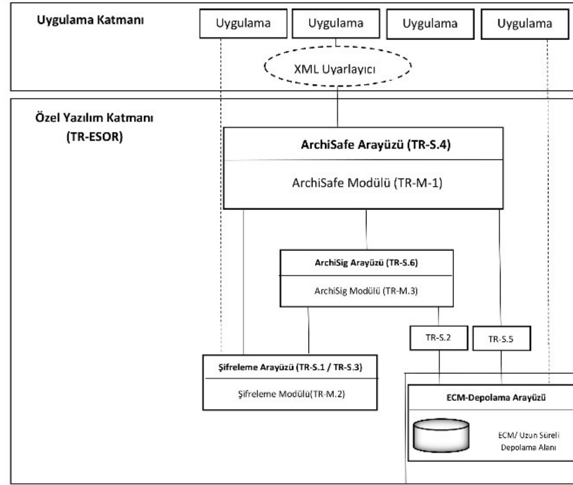
Şekil 4: EDS 1'den EDS 2'ye Belge Transferi
Kaynak: (Deussen vd., 2012, s. 84)

Şekil 4’te görüldüğü üzere; EDS 1'in saklama alanından, Arşiv Nesnesi Tanımlayıcısı (AOID) tarafından tanımlanan e-arşiv belgelerinin EDS 2'nin saklama alanına transferi işlem sırası gösterilmiştir. Burada önemli olan nokta; transferi başlatan kişinin kimlik bilgilerinin doğrulandıktan sonra belgelerin güvenli bir biçimde taşınması için işlemlerin başlamasıdır. İkinci güvenlik önlemi olarak da erişim izinleri, e-imza ve güvenlik sertifikasının doğrulanıp transfer işleminden sonra geride kalan XAIP (XML-AIP) ve AOID (Archive Object Identifier)’lerin silinmesidir.

Tüm bu işlemleri yapılabilmesi için; belgelendirme, imza doğrulama ve şifreleme hizmeti gereklidir. Buna ek olarak, veri şifrelemeyi destekleyen herhangi bir iletim protokolü, XAIP'lerin taşınması için de kullanılmaktadır.

Almanya Bilgi Güvenliği Federal Bürosu Örneği

Almanya Federal Bilgi Güvenliği Bürosu (Bundesamt für Sicherheitin der Informationstechnik -BSI), çeşitli ISO standartlarına ve Alman Federal Arşivleme Yasasına (Bundesarchivgesetz) dayanan dijital olarak imzalanmış belgelerin uzun vadeli korunması için 2011 yılında bir model geliştirmiştir. BSI Uzun Süreli Saklama mimarisi iki ana bölümden oluşmaktadır: Uzun vadeli depolama için BT altyapısı ile veri ve belgeleri arşivleyen veya onlarla çalışan BT uygulamaları. Arşivleme için kullanılan BT altyapısı ise; arşivleme için çeşitli depolama ortamlarını içeren **uzun süreli saklama sistemleri** ile arşivlenmiş belgelerin yönetimi ile ilgili ispat hukuku tarafından gerekli kılınan tam korumayı sağlayan **kriptografik bileşenler içeren özel yazılımlar**dan oluşur (Federal Güvenlik Bilgi Güvenliği Bürosu 2011, 15-16).



Şekil 4: BSI IT Referans Mimarisi
Kaynak: (Federal Office for Information Security, 2011, s. 36)

ArchiSafe Modülü: ArchiSafe Modülü, ticari uygulamalardan ECM/Uzun Süreli Depolama alanına erişimi denetleyen standart ve güvenli bir ağ geçididir. Modülün amacı; gerçek zamanlı ECM/Uzun Süreli Depolama sistemlerinden üst uygulama sistemleri sınırının net bir mantıksal ayrımının gerçekleştirilmesidir. Uygulama sistemlerinin ECM/Uzun Süreli Depolama alanından ayrılmasını ve depolama alanına erişimin etkin ve güvenilir bir şekilde kontrol edilmesini sağlar (Federal Office for Information Security, 2011, s. 38).

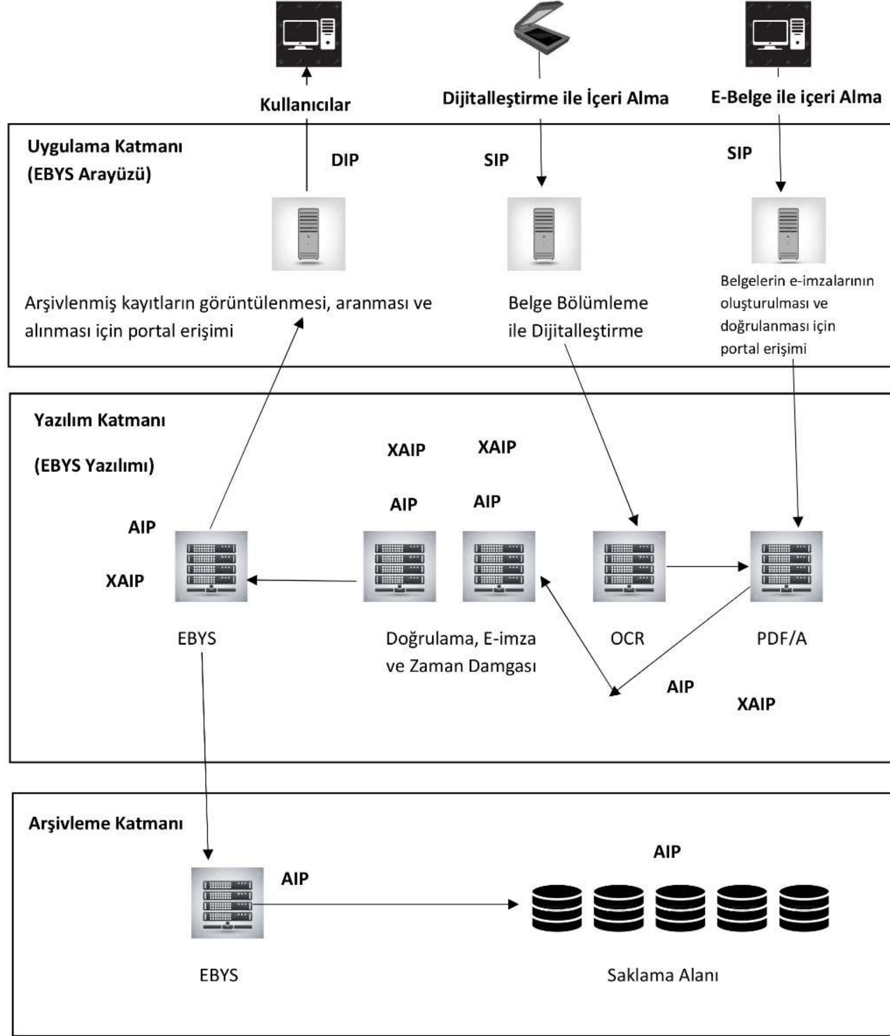
Şifreleme Modülü*:* Şifreleme Modülü, kanıtların korunması için gerekli olan çeşitli şifreleme işlevleri sunar. Bu modül; elektronik imzaların oluşturulması ve doğrulanması için gerekli şifreleme prosedürlerini ve nitelikli zaman damgalarını almak ve doğrulamak için kullanılan mekanizmaları içermektedir. İsteğe bağlı elektronik imzanın oluşturması ve doğrulanması, elektronik sertifikaların tekrar doğrulanması, özel yazılım katmanı için nitelikli zaman damgalarının yanı sıra sertifikasyon ve zaman damgası sağlayıcılarına yönelik arayüzlere erişim için gerekli olan tüm fonksiyonları sağlar (Federal Office for Information Security, 2011, s. 39).

ArchiSig Modülü: ArchiSig Modülü, elektronik imza özelliklerinin korunması ve yenilenmesi, arşivlenen veri nesnelerinin bütünlüğü ve kriptografik delillerin oluşturulması gerekli işlevleri sağlar. Modül, tüm şifreleme fonksiyonları için, Kriptografik Modüle erişir. Bu nedenle, modülün kendisi herhangi bir şifreleme fonksiyonu uygulamak zorunda kalmaz (Federal Office for Information Security, 2011, s. 39).

XML Uyarlayıcı: Uygulamaya özgü veya üst düzey uygulamalarda veriler ve belgeler temelinde depolama için standartlaştırılmış XML tabanlı bir veri biçimi oluşturan uygulama türüne özgü veri dönüştürücüleridir. Ayrıca, XML verilerini uygulamaların içine aktarmayı desteklemektedir. Özel veri formatlarının açık veri formatlarına (örneğin PDF/A) dönüşümünü de sağlar (Federal Office for Information Security, 2011, s. 40).

Enterprise Content Management (ECM) Uzun Süreli Depolama Alanı: Elektronik arşivin veri havuzunu oluşturan modüldür. Arşivlenen veriler ve belgeler burada uzun vadeli depolama ve doluluk için gerekli olan tüm trafik ve idari bilgileri içeren güvenli bir şekilde saklanır. Bunu EBYS bağlamında Repository alanı olarak düşünebiliriz (Federal Office for Information Security, 2011, s. 37).

Entegre Uzun Süreli Korunma Modeli



Şekil 6: OAIS Temelli Uzun Süreli Koruma Hizmetleri Mimarisi

OCR destekli tarayıcılar veya EBYS içerisinde oluşturulan belgelerin SIP paketleri halinde sisteme alınmasından sonra EBYS içerisindeki özel yazılım bloğunda XML paketleri olarak bulunan AIP'ler elektronik olarak imzalanıp zaman damgası aldıktan sonra arşivlenmek üzere "Arşivleme Katmanı"na transfer edilirler. Burada yine AIP paketleri olarak uzun süreli saklama alanında tutulan

belgeler, gerektiğinde sorgulanmak veya okunmak istendiğinde DIP formatında kullanıcılara sunulmak üzere uygulama sunucularına iletilir.

Birçok farklı EBYS yazılımı bulunmakla beraber, genelde hatalar anlık duruma göre şekillendiğinden, hatanın o zamanki durumuna göre işlem yapılamamaktadır. Sürüm atıldığında evrakların bozulması veya görüntülenmemesi gibi bir problemle karşılaşılmamaktadır çünkü sürüm güncelleme işlemleri e-belgeler ile ilgili değil, veritabanları üzerinde olmaktadır. E-belgelerin şifreleme algoritması değişmediğinden belge yapıları sabit kalmaktadır. Belgeler, Repository alanında tutulmakta fakat ayrı bir XML paketi halinde bulunmamaktadır. XML, meta alanlarında oluşacağı için ilgili XML, ihtiyaç olduğunda veritabanından üretilip paketler halinde belgelerin üstverisine eklenmektedir. Veritabanı ve yazılımın içinde bulunan Repository bölümünde bir hasar oluşmadığı sürece bu üstverilere her zaman erişilebilmektedir. İstenmeyen durumların önüne geçmek için de kurumların yedekleme politikaları, felaket kurtarma merkezleri gibi unsurların etkin kullanımı ile sunucuların güvenliğinin sağlanması gerekmektedir (Hamdi Akça, kişisel görüşme, 25.08.2017).

Sonuç

Elektronik Belge Yönetim Sistemlerinde oluşturulan e-belgeler, yaşam döngülerini tamamladıktan sonra herhangi bir özelliğinden ötürü saklanması gerektiğinde sanal depolama alanlarında uzun süreli saklanmaktadır. Uzun süreli saklama mantığında, elektronik depolama ortamında tutulan e-belgelerin birtakım standart ve modellere göre arşivlenmesi gerekmektedir. Genellikle basılı materyalin dijitalleştirildikten sonra bilgisayar ortamında uzun süreli korunması hususunda sistem kriterleri getiren bir model olan OAIS, sahip olduğu bilgi paketleri ile saklama işlevini belirli bir çerçevede yerine getirmektedir. Yapılan görüşmeler sonucunda ülkemizde kullanılan EBYS'lerde uzun süreli saklama açısından herhangi bir model kullanılmamakta olup, saklama mantığı daha çok veritabanlarında belgelerin oldukları gibi (PDF/A formatında) muhafaza edilmesi şeklindedir.

Uzun süreli koruma kapsamında OAIS Referans Modeli temelinde bir e-arşiv sistemini kurmak ve uygulamak için aşağıdakilerin gerçekleşmesi önem arz etmektedir:

- EBYS'nin TS 13298 standartına uygun olarak üretilmesi veya bu standart gereklerini sağlayan kuruluşlardan tedarik edilmesi,
- Kurum özelliklerinin dikkatli bir biçimde analiz edilerek belge envanter yapısının çıkarılması,
- Saklama planlarının Standart Dosya Planı'na göre oluşturulması,

- Mevcut EBYS'ye belge göçü sağlayabilecek EDS destekli bir uygulama sunucusunun entegre edilmesi,
- EBYS'de üretilen veya dış kaynaktan EBYS'ye aktarılan belgelerin SIP paketlerine dönüştürülmesi ve ardından bu paketlerin XML tabanlı AIP paketlerine dönüştürülerek, saklama alanlarında gerektiğinde doğrudan iletime hazır bir şekilde saklanması,
- XAIP paketleri halinde saklama alanlarında bulunan belgelerin, kullanıcılar tarafından çeşitli sorgular yapılarak erişim için çağrıldığında, DIP paketlerine dönüşerek güvenli görüntülemeye imkân tanıması,
- Olası bir felaket senaryosunda Disaster Recovery (Felaket Kurtarma) yapılması, eğer bu yoksa EDS destekli bir başka uygulama sunucusuna belgelerin içerik özellikleri korunarak transferinin sağlanması,
- Doğrulama ve güvenlik yöntemlerinin sürdürülebilirliği için sistemin sürekli güncellemeye açık olması gerekmektedir.

Uzun süreli koruma, her ne kadar bulut arşiv uygulamalarında sıklıkla yapılıyorsa da, OAIS modelinin sanal ve fiziksel sunucular üzerinde de uygulanmasında herhangi bir engel bulunmamaktadır. Ülkemizde geliştirilen EBYS'lerin daha güvenli bir koruma sunması için bahsedilen modele uygun bir uygulama geliştirmeleri veya program güncellemelerini bu doğrultuda yapmaları gerekmektedir.

Modelin EBYS'lerde uygulanmasına dair bir önemli eksikliği de; Standart Dosya Planı'na göre sadece birkaç yıl saklanıp sonrasında imha edilmesi gereken arşiv belgelerine yönelik bir yaklaşım sunmamasıdır. Bunun nedeni, modelin doğası gereği uzun süreli saklama mantığına sahip olmasıdır.

Kaynakça:

Aydın, C. (2010). Elektronik Belgelerin Arşivlenmesi Ve Erişim. Doktora Tezi, Ankara Üniversitesi.

Aydın, C. ve Özdemirci, F. (2011). Elektronik Belgelerin Arşivlenmesinde Gerçekliğin ve Bütünlüğün Korunması. Bilgi Dünyası, 12(1) 105-127.

Breitenstrom, C., Marco, B. ve Klessmann, J. (2008). Elektronische Safes fur Daten und Documente Berlin:Fraunhofer Institut für Offene Kommunikationssysteme.

" Doceō ". Pocket Oxford Latin Dictionary: Latin-English. 3rd ed. 2005

Duranti, L. (2005). The Long-Term Preservation of Accurate And Authentic Digital Data: The Interpares Project, 106-117.

Deussen, P., Eckert, K.P., Strick, L. ve Witaszek, D. (2012). Cloud Concepts for the Public Sector in Germany: Use Cases. Berlin: FOKUS Fraunhofer Institute for Open Communication Systems.

Federal Office for Information Security. (2011). BSI Technical Guideline 03125 on the Preservation of Evidence of Cryptographically Signed Documents. Bonn: Federal Office for Information Security.

ISO 15489-1:2001 (1st ed.). Information and Documentation-Records Management: ISO/TC 46/SC 11 Archives/Records Management.

Janée, G., Methena, J. ve Frew, J. (2008). A Data Model and Architecture for Long-Term Preservation. JCDL '08 Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries, 134-144.

Kandur, H. (2005). Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli. Devlet Arşivleri Genel Müdürlüğü, İstanbul.

Kandur, H. (2011). Türkiye'de Kamu Kurumlarında Elektronik Belge Yönetimi: Mevcut Durum Analizi ve Farkındalığın Artırılması Çalışmaları. Bilgi Dünyası, 12(1), 2-12.

Lavoie, B. (2014). The Open Archival Information System (OAIS) Reference Model Introductory Guide (2nd ed.). DPC Technology Watch Report: Digital Preservation Coalition.

Millar, L. (2009). Glossary of Terms Training in Electronic Records Management. International Records Management Trust, United Kingdom.

Moses, R. P. (2005). A Glossary of Archival and Records Terminology. The Society of American Archivists. Chicago.

Odabaş, H. (2005). Belge Yönetimi ve Türkiye'de Belge Yönetimi Gereksinimi. Bilgi Dünyası 6 (1), 36-57

Paquet, E. ve Viktor, H. L. (2007). Long-Term Preservation of 3D Cultural Heritage Data Related to Architectural Sites. International Society for Photogrammetry and Remote Sensing Proceedings 36 (5).

Potthoff, J., Marius W. ve Sebastian, R. (2013). Data Management According to the Good Scientific Practice. In The Fifth International Conference on Advances in Databases, Knowledge, and Data Applications, p.27–32.

Preserving Digital Information. (1996). Report of the Task Force on Archiving Digital Information Commissioned by The Commission on Preservation and Access and The Research Libraries Group. May 1, 1996. 18.08.2017 tarihinde https://www.clir.org/pubs/reports/pub63watersgarrett.pdf adresinden erişildi.

Rounds, S. ve Horton, R. (2004). Electronic Records Management Guidelines. State Archives Department: Minnesota Historical Society.

Sawyer, Don (2001). The Open Archival Information System and the NSSDC. 22.08.2017 tarihinde https://nssdc.gsfc.nasa.gov/nssdc_news/dec00/oais.html adresinden erişildi.

Shepherd, E. (1994). Managing Electronic Records. Records Management Journal, 4(1), p. 39-49.

Sproull, R. F. ve Eisenberg, J. (2005). Building An Electronic Records Archive At The National Archives And Records Administration: Recomendation For A Long-Term Strategy. Washington DC: National Academies Press.

The Consultative Committee for Space Data Systems. (2012). Reference Model For An Open Archival Information System (OAIS) Recommended Practice CCSDS 650.0M-2 Magenta Book. Washington, DC: Space Operations Mission Directorate.

Tonta, Y. (2002). İnternet ve Elektronik Bilgi Yönetimi. 23.08.2017 tarihinde http://yunus.hacettepe.edu.tr/~tonta/courses/fall2002/kut655/01-eby-version2.pdf adresinden erişildi.



e-ISBN: 978-605-61009-9-4



Ankara Üniversitesi Basımevi
http://basimevi.ankara.edu.tr

Para ile satılmaz.